IMAGE ADAPTIVE WATERMARKING USING WAVELET TRANSFORM

A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

MASTER OF TECHNOLOGY

IN

ELECTRONICS SYSTEM AND COMMUNICATION

By

Ms. T MITA KUMARI

Department of Electrical Engineering

National institute of Technology

Rourkela-769008

2007

IMAGE ADAPTIVE WATERMARKING USING WAVELET TRANSFORM

A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

MASTER OF TECHNOLOGY

IN

ELECTRONICS SYSTEM AND COMMUNICATION

By

Ms. T MITA KUMARI

Under the Guidance of

Dr. SUPRAVA PATNAIK

Department of Electrical Engineering

National institute of Technology

Rourkela-769008

2007

National institute of Technology
Rourkela

CERTIFICATE

This is to certify that the thesis entitled "**Image Adaptive Watermarking using Wavelet Transform**" submitted by **Ms. T Mita Kumari**, in partial fulfillment of the requirements for the award of Master of Technology in the Department of Electrical Engineering, with specialization in '**Electronics System and Communication'** at National Institute of Technology, Rourkela (Deemed University) is an authentic work carried out by her under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University/Institute for the award of any Degree or Diploma.

Date:

Dr. Suprava Patnaik
Asst. Professor
Department of Electrical Engineering
NATIONAL INSTITUTE OF TECHNOLOGY
Rourkela-769008

ACKNOWLEDGEMENTS

On the submission of my thesis report of "**Image Adaptive Watermarking Using Wavelet Transform**", I would like to extend my gratitude & my sincere thanks to my supervisor **Dr. Suprava Patnaik**, Asst. Professor, Department of Electrical Engineering for her constant motivation and support during the course of my work in the last one year. I truly appreciate and value her esteemed guidance and encouragement from the beginning to the end of this thesis. I am indebted to her for having helped me shape the problem and providing insights towards the solution.

I express my gratitude to Dr.P.K.Nanda, Professor and Head of the Department, Electrical Engineering for his invaluable suggestions and constant encouragement all through the thesis work.

I will be failing in my duty if I do not mention the laboratory staff and administrative staff of this department for their timely help.

I would like to thank all whose direct and indirect support helped me completing my thesis in time.

This thesis would have been impossible if not for the perpetual moral support from my family members, and my friends. I would like to thank them all.

T Mita Kumari

M.Tech (Electronics System and Communication)

CONTENTS

ABSTRACT

The availability of versatile multimedia processing software and the far-reaching coverage of the interconnected networks have facilitated flawless copying, manipulations and distribution of the digital multimedia (digital video, audio, text, and images). The ever-advancing storage and retrieval technologies have also smoothed the way for large-scale multimedia database applications. However, abuses of these facilities and technologies pose pressing threats to multimedia security management in general, and multimedia copyright protection and content integrity verification in particular. Although cryptography has a long history of application to information and multimedia security, the undesirable characteristic of providing no protection to the media once decrypted has limited the feasibility of its widespread use. For example, an adversary can obtain the decryption key by purchasing a legal copy of the media but then redistribute the decrypted copies of the original .In response to these challenges; digital watermarking techniques have been proposed in the last decade. Digital watermarking is the procedure whereby secret information (the watermark) is embedded into the host multimedia content, such that it is: (1) hidden, i.e., not perceptually visible; and (2) recoverable, even after the content is degraded by different attacks such as filtering, JPEG compression, noise, cropping etc. The two basic requirements for an effective watermarking scheme, imperceptibility and robustness, conflict with each other.

The main focus of this thesis is to provide good tradeoff between perceptual quality of the watermarked image and its robustness against different attacks. For this purpose, we have discussed two robust digital watermarking techniques in discrete wavelet (DWT) domain. One is fusion based watermarking, and other is spread spectrum based watermarking. Both the techniques are image adaptive and employ a contrast sensitivity based human visual system (HVS) model. The HVS models give us a direct way to determine the maximum strength of watermark signal that each portion of an image can tolerate without affecting the visual quality of the image.

In fusion based watermarking technique, grayscale image (logo) is used as watermark. In watermark embedding process, both the host image and watermark image are transformed into DWT domain where their coefficients are fused according to a series combination rule that take into account contrast sensitivity characteristics of the HVS. The method repeatedly merges the

watermark coefficients strongly in more salient components at the various resolution levels of the host image which provides simultaneous spatial localization and frequency spread of the watermark to provide robustness against different attacks. Watermark extraction process requires original image for watermark extraction.

In spread spectrum based watermarking technique, a visually recognizable binary image is used as watermark. In watermark embedding process, the host image is transformed into DWT domain. By utilizing contrast sensitivity based HVS model, watermark bits are adaptively embedded through a pseudo-noise sequence into the middle frequency sub-bands to provide robustness against different attacks. No original image is required for watermark extraction.

Simulation results of various attacks are also presented to demonstrate the robustness of both the algorithms. Simulation results verify theoretical observations and demonstrate the feasibility of the digital watermarking algorithms for use in multimedia standards.

LIST OF FIGURES

LIST OF ACRONYMS

ACF	Auto Covariance Function
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CD	Compact Disc
EZW	Embedded Zero Wavelet Tree
DAB	Digital Audio Broadcasting
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DSP	Digital Signal Processing
DWT	Discrete Wavelet Transform
HVS	Human Visual System
IDWT	Discrete Wavelet Transform
JND	Just Noticeable Difference
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MPEG	Moving Picture Experts Group
MSE	Mean Square Error
PN	Pseudo Noise
PSNR	Peak Signal to Noise Ratio
QF	Quality Factor
SNR	Signal to Noise Ratio

CHAPTER 1

INTRODUCTION

Introduction

Watermarking Requirements

Watermarking Applications

Contribution of the thesis and Chapter organization

1.1 INTRODUCTION

In recent years, digital multimedia technology has shown a significant progress. This technology offers so many new advantages compared to the old analog counterpart. The advantages during the transmission of data, easy editing any part of the digital content, capability to copy a digital content without any loss in the quality of the content and many other advantages in DSP, VLSI and communication applications have made the digital technology superior to the analog systems. Particularly, the growth of digital multimedia technology has shown itself on Internet and wireless applications. Yet, the distribution and use of multimedia data is much easier and faster with the great success of Internet. The great explosion in this technology has also brought some problems beside its advantages. However, abuses of these facilities and technologies pose pressing threats to multimedia security management in general, and multimedia copyright protection and content integrity verification in particular. Although cryptography has a long history of application to information and multimedia security, the undesirable characteristic of providing no protection to the media once decrypted has limited the feasibility of its widespread use. For example, an adversary can obtain the decryption key by purchasing a legal copy of the media but then redistribute the decrypted copies of the original .In response to these challenges, digital watermarking schemes have been proposed in the last decade.

A watermark [1], a secret imperceptible signal, is embedded into the original data in such a way that it remains present as long as the perceptible quality of the content is at an acceptable level. The owner of the original data proves his/her ownership by extracting the watermark from the watermarked content in case of multiple ownership claims. Digital watermark may be comprised of copyright or authentication codes, or a legend essential for signal interpretation. The existence of these watermarks with in a multimedia signal goes unnoticed except when passed through an appropriate detector. Common types of signals to watermark are still images, audio, and digital video.

As an example of the usefulness of watermarking, let us consider a simple scenario: Newspaper X publishes a photograph, for which it claims exclusive rights. Newspaper Y, also claiming to be the exclusive owner, publishes the same photograph after copying it from X. Without any special protection mechanism, X cannot prove that it is the rightful owner of the photograph. However, if X watermarks the photograph before publication (that is, X embeds a

hidden message that identifies it as its legitimate owner), and is able to detect the watermark later in the illegally distributed copy, it will be able to supply proof of ownership in a court of law. On the other hand, to prevent detection of the watermark, Y may try to remove it from the picture by distorting the picture. That is, Y may attempt to attack the watermark so as to render it undetectable, without significantly degrading the quality of the image or affecting its commercial value. Careful design of the watermarking system can prevent this from happening. There have been many instances of disputes or litigations on the intellectual ownership of multimedia data. A copyright violations lawsuit that received extensive publicity in the early 2000's, was that against Napster .Napster was essentially a centralized database which allowed millions of users to freely distribute music files in a peer-to-peer network. The music files were un-watermarked and compressed in such a way that the quality of the reproduced music was very close to that of a Compact Disc (CD recording). However, all copyright information that normally accompanies the music written on a CD was lost. As a result, it was not an easy task for the music companies to prove that unauthorized distribution was indeed taking place through Napster. A watermarking scheme robust to compression would have provided additional ammunition to the music industry, as the copyright information would have been inseparable from the music itself. Due to its significance, the watermarking field has grown tremendously over the last years. There are numerous articles [2, 3, 4, 5, and 6] that explain the basics of watermarking, explore its practical applications, and evaluate the performance of various schemes under a variety of attacks.

1.2 WATERMARKING SYSTEM

In this thesis, work has been carried out on digital watermarking. Throughout the rest of the report, watermarking refers to digital watermarking. To avoid the unauthorized distribution of images or other multimedia property, various solutions has been proposed. Most of them make unobservable modifications to images that can be detected afterwards. Such image changes are called watermarks. Watermarking is defined as adding (embedding) a watermark signal to the host signal. The watermark can be detected or extracted later to make an assertion about the object. A general scheme for digital watermarking is given in Figure 1.1. The watermark message can be a logo picture, sometimes a visually recognizable binary picture or it can be binary bit stream. A watermark is embedded to the host data by using a secret key at the embedder.

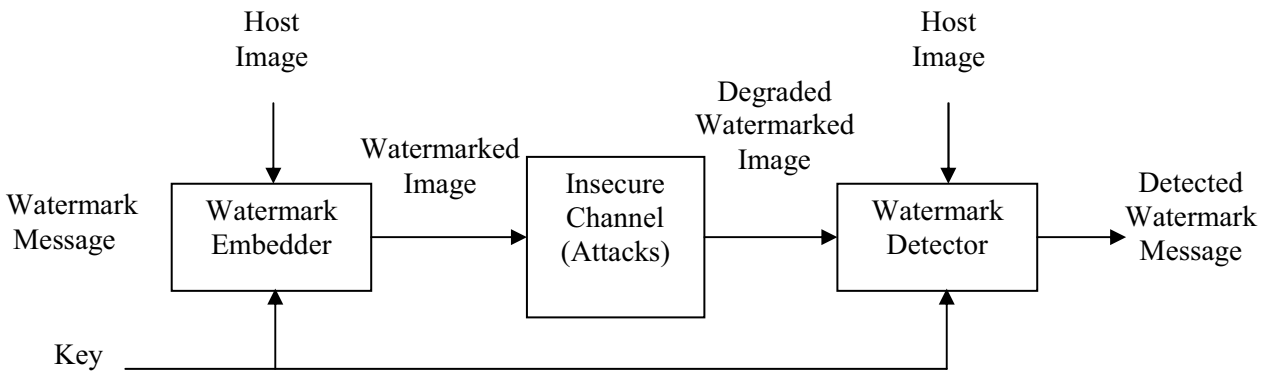


Fig. 1.1 A Digital Watermarking System

The information embedding routine imposes small signal changes, determined by the key and watermark, to generate the watermarked signal. Only the owner of the data knows the key and it is not possible to remove the message from the data without the knowledge of the key. Then, the watermarked image passes through the transmission channel. The transmission channel includes the possible attacks, such as lossy compression, geometric distortions, any common signal processing operation and digital-analog and analog to digital conversion, etc. After the watermarked image passes through these possible operations, the message is tried to be extracted at the watermark detector. The decoding process can itself performed in two different ways. In one process the presence of the original unwatermarked data is required and other blind decoding is possible. The extracted watermark is compared with the original watermark (i.e. the watermark that was initially embedded) by a comparator function and binary output decision is generated. The comparator is basically a correlator. Depending on the comparator output it can be determined if the data is authentic or not. If the comparator output is greater than equal to a threshold then the data is authentic else it is not authentic.

A watermark is detectable or extractable to be useful. Depending on the way the watermark is inserted and depending on the nature of the watermarking algorithm, the method used can involve very distinct approaches. In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call watermark extraction. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call watermark detection. It should be noted that watermark extraction can prove ownership whereas watermark detection can only verify ownership.

1.3 WATERMARKING REQUIREMENTS

Watermark by itself is not sufficient to prevent abuses unless a proper protection protocol is established. The exact properties that a watermarking algorithm must satisfy cannot be defined exactly without considering the particular application scenario; the algorithm has to be used in. For example, in the video indexing application, evaluating the robustness of a watermarking scheme to any signal processing is meaningless, since there is no case that the video passes through some signal processing operation. In the covert communication application, it is better to use a watermarking scheme that does not need the original data during the watermark detection process, if real TV broadcasting is used as the communication channel, while most of the watermarking schemes in other applications need the original data during the detection process. If the application is the copyright protection, the owner of the original data may wait for several days to insert/detect watermark, if the data is valuable for the owner. On the other hand, in a broadcast monitoring application, the speed of the watermark detection algorithm should be as fast as the speed of real time broadcasting. As a result, each watermarking application has its own requirements and the efficiency of the watermarking scheme should be evaluated according to these requirements.

Each watermarking application has its own specific requirement and the design is complicated by the conflicting interdependence of the different requirements. It makes it difficult to study all aspects simultaneously but it appears also hard to successfully isolate the different constraints. The main requirements which should be fulfilled by a watermarking scheme are imperceptibility, robustness, capacity

1.3.1 Imperceptibility

Watermarking algorithm must embed the watermark such that this does not introduce any perceptible artifacts into the host data and not degrade the perceived quality of the underlying host data. A watermark-embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark [2]. Even the smallest modification in the host data may become apparent, however, when the original data is compared directly with the watermarked data. Since users of watermarked data normally do not have access to the original data, they cannot perform this comparison. Therefore, it may be sufficient that the

modifications in the watermarked data go unnoticed as long as the data are not compared with the original data [6].

1.3.2 Robustness

Robustness refers to the ability to detect the watermark, even if the quality of the host data is degraded, intentionally (malicious) or unintentionally (non-malicious). In general, there should be no way in which the watermark can be removed or altered without sufficient degradation of the perceptual quality of the host data so as to render it unusable.

The Exact level of robustness the hidden data must posses cannot be specified without considering a particular application. Qualitative robustness level encompassing most of the situations encountered in practice have been discussed below.

Secure Watermarking:

In this case, mainly dealing with copyright protection, ownership verification or any other security-oriented application, the watermark must survive both no-malicious as well as malicious manipulations. In secure watermarking, the loss of the hidden data should be obtainable only at the expense of a significant degradation of the quality of the host signal. When considering malicious manipulation it has to be assumed that attackers known the watermarking algorithm and thereby they can conceive ad-hoc watermark removal strategies. The security must lie on the choice of key. The watermarking algorithm has truly secure if knowing the exact algorithms for embedding and extracting the watermark does not help unauthorized party to detect the presence of the watermark. As to non- malicious manipulations, they include a huge variety of digital and analog processing tools, including lossy compression, linear and non-linear filtering, cropping editing, scaling, D/A and A/D conversions, analog duplications, noise addition, and many others that apply only to particular type. Thus in the image case, we must considering zooming and shrinking, rotation, contrast, enhancement histogram manipulation, row/ column removal or exchange, in the case of video we must taken into account frame removal, frame exchange, temporal filtering, temporal re-sampling, finally robustness of an audio watermark, may imply robustness against echo addition, multi-rate processing, and pitch scaling. It is though important to point out that even the most secure system does not need to perfect the contrary, it is only needed that a high enough degree of security is reached. In other words, watermark breaking

does not need to be impossible (which probably will never be the case), but only difficult enough.

Robust watermarking:

In this case it is required that the watermark be resistant only against non-malicious manipulations. Robust watermarking is less demanding than secure watermarking. Application fields in robust watermarking include all the situations in which it is unlikely that someone purposely manipulates the host data with the intention to remove the watermark. The application scenario is such that the normal use of data comprise of several kinds of manipulations, which must not damage the hidden data. Even in copyright protection applications, the adoption of robust watermarking instead of secure watermarking may be allowed due to the use of a copyright protection protocol in which all the involved actors are not interested in removing the watermark.

Semi-fragile watermarking:

Watermark is semi-fragile if it survives a limited well specified, set of manipulations, leaving the quality of the host document virtually intact. In some applications robustness is not a major requirement, mainly because the host signal is not intended to undergo any manipulations, but a very limited number of minor modifications such as moderate lossy compressions, or quality enhancement. This is the case of data labeling for improved actual retrieval, in which the hidden data is only needed to retrieve the host data from archive, and thereby it can be discarded once the data has been correctly assessed. Usually data is archived in compressed format, and that the watermark is embedded prior to compression. In this case the watermark needs to be robust against lossy coding.

Fragile watermarking:

A watermark is said to be fragile if the information hidden with in the host data is lost or irremediably altered as soon as any modification is applied to the host signal. Such a loss of information may be global, i.e. no part of watermarking can be recovered, or local i.e. only part of the watermark is damaged. The main application of fragile watermarking is data authentication, where watermark loss or alternation is taken as evidence that the data has been

tampered with. The recovery of the information content within the data demonstrates authentic un-tampered data.

Robustness against signal distortion is better achieved if the watermark is placed in perceptually significant part of the signal. This is particularly evident in the case of lossy compression algorithm, which operates by discarding perceptually insignificant data. Watermark hidden within perceptually insignificant data are likely not to survive compression. Achieving watermark robustness, and, to a major extent, watermark security is one of the main challenges watermarking researches are facing with. Nevertheless its importance has sometimes been over estimated at the expense of other very important issues as watermark capacity and protocol level analysis.

1.3.3 Capacity

The capacity requirement of the watermarking scheme refers to be able to verify and distinguish between different watermarks with a low probability of error as the number of differently watermarked versions of an image increases [7].

The requirements listed above are all related to each other. The mutual dependencies between the basic requirements are shown in Fig. 1.2. For instance, a very robust watermark can

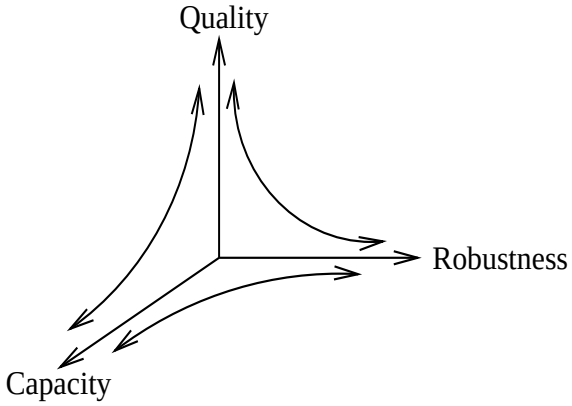


Fig. 1.2 Mutual dependencies between the basic requirements

be obtained by making many large modifications to the host data for each bit of the watermark. Large modifications in the host data will be noticeable, however, and many modifications per watermark bit will limit the maximum amount of watermark bits that can be stored in a data object. The robustness of the watermarking method increases, the capacity also increases where

the imperceptibility decreases. The security of a watermark influences the robustness enormously. If a watermark is not secure, it cannot be a very robust. Hence, a tradeoff should be considered between the different requirements so that an optimal watermark for each application can be developed.

1.4 WATERMARKING APPLICATIONS

Although the main motivation behind the digital watermarking is the copyright protection, its applications are not that restricted. There is a wide application area of digital watermarking, including broadcast monitoring, fingerprinting, authentication and covet communication [5, 8]. For secure applications a watermark is used for following purposes:

1. Copyright Protection: For the protection of intellectual property, the data owner can embed a watermark representing copyright information in his data. This watermark can prove his ownership in court when someone has infringed on his copyrights.
2. Fingerprinting: To trace the source of illegal copies, the owner can use a fingerprinting technique. In this case, the owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in the data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties.
3. Broadcast Monitoring: By embedding watermarks in commercial advertisements, an automated monitoring system can verify whether advertisements are broadcasted as contracted. Not only commercials but also valuable TV products can be protected by broadcast monitoring. The same process can also be used for video and sound clips. Musicians and actors may request to ensure that they receive accurate royalties for broadcasts of their performances.
4. Data Authentication**:** The authentication is the detection of whether the content of the digital content has changed. As a solution, a fragile watermark embedded to the digital content indicates whether the data has been altered. If any tampering has occurred in the content, the same change will also occur on the watermark. It can also provide information about the part of the content that has been altered

5. Copy Protection: The information stored in a watermark can directly control digital recording devices for copy protection purposes. In this case, the watermark represents a copy-prohibit bit and watermark detectors in the recorder determine whether the data offered to the recorder may be stored or not.
6. Covert Communication: The watermark, secret message, can be embedded imperceptibly to the digital image or video to communicate information from the sender to the intended receiver while maintaining low probability of intercept by other unintended receivers.

For non-secure applications a watermark is used for following purposes:

1. Indexing: Indexing of video mail, where comments can be embedded in the video content; indexing of movies and news items, where markers and comments can be inserted that can be used by search engines.
2. Medical Safety: Embedding the date and the patient's name in medical images could be a useful safety measure.
3. Data Hiding: Watermarking techniques can be used for the transmission of secrete private messages. Since various governments restrict the use of encryption services, people may hide their messages in other data.

Although not yet widely recognized as such, bandwidth-conserving hybrid transmission is yet another information embedding application, offering the opportunity to re-use and share existing spectrum to either backwards-compatibility increase the capacity of an existing communication network, i.e., a "legacy" network, or allow a new network to be backwards-compatibility overlaid on top of the legacy network. In this case the host signal and embedded signal are two different signals that are multiplexed, i.e., transmitted simultaneously over the same channel in the same bandwidth, the host signal being the signal corresponding to the legacy network. Unlike in conventional multiplexing scenarios, however, the backwards compatibility requirement imposes a distortion constraint between the host and composite signals.

So-called hybrid in-band on-channel digital audio broadcasting (DAB) is an example of such a multimedia application where one may employ information embedding methods to backwards-compatibility upgrade the existing commercial broadcast radio system. In this application one would like to simultaneously transmit a digital signal with existing analog (AM and/or FM) Commercial Broadcast radio without interfering with conventional analog reception. Thus, the analog signal is host signal, and the digital signal is the watermark. Since embedding

does not degrade the host signal too much, conventional analog receivers can demodulate the analog host signal. This embedded signal may be all or part of a digital audio signal, an enhancement signal used to refine the analog signal, or supplemental information such as station identification.

1.5 CONTRIBUTION OF THE THESIS AND CHAPTER ORGANIZATION

This thesis addresses the issues regarding Digital watermarking and its applications. The work included in this thesis aims to provide a good trade-off between perceptual quality of the watermarked image and its robustness to different attacks, by developing adaptive watermarking algorithms using wavelet transform and human visual system (HVS) model. Two watermarking algorithms have been discussed in this work. The first one is multiresolution fusion based watermarking. The second one is spread spectrum based watermarking technique. The rest of the thesis is organized as follows:

The different watermarking attacks, and performance measurements which evaluates the watermarking algorithms is presented in **Chapter 2**. The literature review on digital watermarking is also summarized in this chapter.

Fusion based watermarking technique has been discussed in **Chapter 3**.The technique requires host signal for watermark extraction and employs image fusion principle to embed both small grayscale and binary watermarks. Simulation and analysis demonstrates the improved performance of the technique to a wider variety of attacks such as JPEG compression, filtering, additive noise, and cropping.

Spread spectrum based watermarking technique has been discussed in **Chapter 4**. The technique is a blind technique and watermark bits are embedded through a pseudo noise sequence. Simulation and analysis demonstrates the robustness of the technique to variety of attacks.

Finally **Chapter 5** presents the concluding remark, with scope for further research work.

CHAPTER 2

WATERMARKING ATTACKS AND PERFORMANCE MEASUREMENTS

Introduction

Classification of attacks

Performance measures of watermarking algorithms

Literature review

Chapter summary

2.1 INTRODUCTION

To win each campaign, a general needs to know about both his opponent's as well as his own troops. Attacks aim at weakening the watermarking algorithm. The purpose of any watermark-embedding algorithm is to provide some degree of security and the purpose of any attack is to negate that purpose. Hence the compilation of a report on watermarking is incomplete without a mention of watermarking attacks. Study of watermarking algorithm enable to:

- Identify weakness of the watermarking algorithm
- Propose improvement of the watermarking algorithm
- Study effects of current technology on watermark

In watermarking terminology, an attack is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. The processed watermarked data is then called attacked data.

Watermarking is treated as a communication problem, in which the owner attempts to communicate over a hostile channel, where the non-intentional and the intentional attacks from the channel. The owner tries to communicate as much watermark information as possible while maintaining a sufficient high data quality, contrary, and an attacker tries to impair watermark communication while impairing the data quality as little as possible. Therefore, digital watermarking scenarios can be considered as a game between the owner and attacker. Continuing with the analogy of watermarking as a communication system, some researchers have chosen to work on modeling and resisting attacks on the watermark. They work on the philosophy that the more specific the information known about the possible attacks, the better we can design systems to resist it.

2.2 CLASSIFICATION OF ATTACKS

Attacks can be broadly classified as non-malicious (unintentional) such as compression of a legally obtained, watermarked image or video files and malicious such as an attempt by a multimedia pirate to destroy the embedded information and prevent tracing of illegal copies of watermarked digital video. Watermarking systems utilized in copy protection or data authentication schemes are especially susceptible to malicious attacks. Non-malicious attacks usually come from common signal processing operations done by legitimate users of the watermarked materials.

2.2.1 Malicious attacks

An attack is said to be malicious if its main goal is to remove or make the watermark unrecoverable. Malicious attacks can be further classified into two different classes.

Blind: A malicious attack is said to be blind if it tries to remove or make the watermark unrecoverable without exploiting knowledge of the particular algorithm that was used for watermarking the asset. For example, copy attack that estimates the watermark signal with aim of adding it to another asset.

Informed: A malicious attack is said to be informed if it attempts to remove or make the watermark unrecoverable by exploiting knowledge of the particular algorithm that was used for watermarking the asset. Such an attack first extracts some secrete information about the algorithm from publicly available data and then based on this information nullifies the effectiveness of the watermarking system.

Examples of malicious attacks:

- Printing and Rescanning
- Watermarking of watermarked image (re-watermarking)
- Collusion: A number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an un-watermarked copy of the image (by averaging all the watermarked images).
- Forgery: A number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.
- IBM attack [9]: It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.

2.2.2 Non-Malicious attacks

An attack is said to be non-malicious if it results from the normal operations that watermarked data or any data for that matter has to undergoes, like storage, transmission or fruition. The nature and strength of these attacks are strongly dependent on the application for which the watermarking system is devised.

Examples of non-malicious attacks:

- Lossy Compression: This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark insertion task in the same domain where the compression takes place. Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data.
- Geometric Distortions: Geometric distortions are specific to images videos and include such operations as rotation, translation, scaling and cropping.
- Common Signal Processing Operations: Common signal processing operation includes such operations such as linear filtering such as high pass and low pass filtering, non linear filtering such as median filtering, D/A Conversion, A/D conversion, re-sampling, re-quantization, dithering distortion, addition of a constant offset to the pixel values, addition of Gaussian and Non Gaussian noise, local exchange of pixels.

The existing attacks can be categorized into four classes of attacks [10]: removal attacks, geometric attacks, cryptographic attacks, and protocol attacks.

2.2.3 Removal attacks

Removal attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm, e.g., without the key used for watermark embedding. That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. This category includes denoising, quantization (e.g., for compression), re-modulation, and collusion attacks. Not all of these methods always come close to their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly. Sophisticated removal attacks try to optimize operations like de-noising or quantization to impair the embedded watermark as much as possible while keeping the quality of the attacked document high enough. Usually, statistical models for the watermark and the original data are exploited within the optimization process. Collusion attacks are applicable when many copies of a given data set, each signed with a key or different watermark, can be obtained by an attacker or a group of attackers. In such a

case, a successful attack can be achieved by averaging all copies or taking only small parts from each different copy. Recent results show that a small number of different copies, e.g., about 10, in the hand of one attacker can lead to successful watermark removal.

2.2.4 Geometric attacks

In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained. However, the complexity of the required synchronization process might be too great to be practical. For image watermarking, the most known benchmarking tools, Unzign and Stirmark, integrate a variety of geometric attacks. Unzign introduces local pixel jittering and is very efficient in attacking spatial domain watermarking schemes. Stirmark introduces both global and local geometric distortions. We give a few more details about these attacks later in this paper. However, most recent watermarking methods survive these attacks due to the use of special synchronization techniques. Robustness to global geometric distortions often relies on the use of either a transform invariant domain (Fourier-Melline) or an additional template or of specially designed periodic watermarks whose auto-covariance function (ACF) allows estimation of the geometric distortions. However, as will be discussed below, the attacker can design dedicated attacks exploiting knowledge of the synchronization scheme. Robustness to global affine transformations is more or less a solved issue. However, resistance to the local random alterations integrated in Stirmark still remains an open problem for most commercial watermarking tools. The so-called random bending attack in Stirmark exploits the fact that the human visual system is not sensitive against local shifts and affine modifications. Therefore, pixels are locally shifted, scaled, and rotated without significant visual distortion. However, it is worth noting that some recent methods are able to resist against this attack.

2.2.5 Cryptographic attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is the brute-force search for the embedded secret information. Another attack in this category is the so-called Oracle attack, which can be used to create a non-watermarked signal when a watermark detector device is available. Practically, application of these attacks is restricted due to their high computational complexity.

2.2.6 Protocol attacks

Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks [9]. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data. It has been shown that for copyright protection applications, watermarks need to be non-invertible. The requirement of non-invertibility of the watermarking technology implies that it should not be possible to extract a watermark from a non-watermarked document. A solution to this problem might be to make watermarks signal-dependent by using one-way functions. Another protocol attack is the copy attack. In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data. The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor the knowledge of the watermarking key. Again, signal-dependent watermarks might be resistant against the copy attack.

2.3 PERFORMANCE MEASURES OF WATERMARKING ALGORITHMS

The success of watermarking algorithm is evaluated based on a series of measures [11]. Because of the psychological nature of the problem not all criteria are quantitative in nature. Although only some factors are appropriate for a given application, we present all the most popular metrics below to highlight the character of good watermarking scheme. Without loss of generality, we assume the host and watermarked signals are images.

1. **Perceptual Quality:** Perceptual quality refers to the imperceptibility of embedded watermark data within the host signal. In most applications, it is important that the watermark is undetectable to a listener or viewer. This ensures that the quality of the host signal is not perceivably distorted; the peak signal-to-noise ratio (PSNR) of the watermarked signal versus the host signal was used as a quality measure. The PSNR is defined as :

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$
$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(X(m,n) - X_w(m,n))^2 \qquad 2.1$$

in units of dB, where X is host signal, w is the watermark X_w is the watermarked signal MN, is the total number of pixels in X or X_w.

2. **Correlation Coefficients:** To measure the similarity between embedded and extracted watermarks, the following normalized correlation coefficients is defined as:

$$r = \frac{\sum_m \sum_n w(m,n)\hat{w}(m,n)}{\sqrt{\left(\sum_m \sum_n w^2(m,n)\right)}\sqrt{\left(\sum_m \sum_n \hat{w}^2(m.n)\right)}} \qquad 2.2$$

where w and $\hat{w}$ are the embedded and extracted watermarks, respectively.

3. **Bit Rate:** Bit rate refers to the amount of watermark data that may be reliably embedded within a host signal per unit of time or space, such as bits per second or bits per pixel. A higher bit rate may be desirable in some applications in order to embed more copyright information. In this study, reliability was measured as the bit error rate (BER) of extracted watermark data. For embedded and extracted watermark sequences of length B bits, the BER (in percent) is given by the expression as:

$$BER = \frac{100}{B}\sum_{n=0}^{B-1}\begin{cases}1 & \hat{w}(n) \neq w(n)\\ 0 & \hat{w}(n) = w(n)\end{cases} \qquad 2.3$$

4. **Computational Complexity:** Computational complexity refers to the processing required to embed watermark data into a host signal, and / or to extract the data from the signal. Algorithm complexity is important to know, for it may influence the choice of implementation structure or DSP architecture. Although there are many ways to measure complexity, such as complexity analysis (or "Big-0' analysis), for practical applications more quantitative values are required.

2.4 LITERATURE REVIEW

Digital watermarking is a prominent field of research and many researchers have suggested a large number of algorithms and compared. The main thrust on all such algorithms is to hide secrete information (watermark) in host signal in such a way that it provides good tradeoff between imperceptibility and robustness against different attacks. This section presents several types of digital watermarking techniques found in the academic literature. We do not give an exhaustive review of the area, but provide an overview of established approaches. Existing digital watermarking techniques are broadly classified into two categories depending on the domain of watermark insertion: spatial domain and frequency domain techniques.

The earlier watermarking techniques are almost spatial based approach. In spatial domain the watermark is embedded into the host image by directly modifying the pixel values, i.e. simplest example is to embed the watermark in the least significant bits (LSBs) of image pixels [1]. Spatial domain watermarking is easy to implement and requires no original image for watermark detection. However, it often fails under signal processing attacks such as filtering and compression and having relative low-bit capacity. A simple image cropping operation may eliminate the watermark. Besides, the fidelity of the original image data can be severely degraded since the watermark is directly applied on the pixel values.

In contrast to the spatial-domain-based watermarking, frequency-domain based techniques can embed more bits of watermark and are more robust to attack; thus, they are more attractive than the spatial-domain-based methods, because the watermark information can be spread out to the entire image. As to the frequency transform, there are DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), and DWT (Discrete Wavelet Transform). J.J.K.O'Runaidh *et al.* [12] uses phase of the discrete Fourier transform to embed the watermark. They used the fact that phase is more important than the amplitude of the DFT values for the intelligibility of an image. Watermarking technique proposed by J.J.K.O'Runaidh *et al*. [13] use DFT amplitude modulation because of its translation or shift invariant property. Because cyclic translation of the image in the spatial domain does not affect the DFT amplitude, the watermark embedded in this domain will be translation invariant. However, embedding watermark in host image by DFT is suffering from the JPEG attacks. The watermarking technique using DCT and DWT provides extra robustness to different attacks.

I.J. Cox *et el.* [14] proposed a watermarking technique by taking DCT of entire image. The method involves adding watermark to the *N* lowest frequency non-dc DCT coefficients of the host image where *N* is the length of the watermark sequence of zero mean and unit variance by using the following equation:

$$F_w^{DCT}(w_1, w_2) = F^{DCT}(w_1, w_2)(1 + aw(i)) \qquad 2.4$$

where $F^{DCT}(w_1, w_2)$ and $F_w^{DCT}(w_1, w_2)$ are the DCT coefficients of the host image and watermarked image respectively, *a* is the scaling parameter, and *w(i)* is the i^{th} watermark element. This algorithm is one of the earliest attempts at providing image adaptability in the watermark embedding scheme. This is due to the fact that the watermark strength depends on the intensity of the DCT coefficients of the original image. In this way, the watermark signal can be quite strong in the DCT coefficients with large intensity values and is attenuated in the areas with small DCT coefficients. F.M. Boland *et el.* [15] proposed a method which also modulates the coefficients but uses a one-dimensional bipolar binary sequence. The marking procedure consists of sorting the DCT coefficients of the image according to their absolute magnitude. The watermark is then added to the *N* largest AC coefficients. Inserting the watermark into the perceptually significant components and adapting the watermark strength by the strength of the DCT component provides a watermark that is quite robust and transparent. However, because the DCT is obtained on the entire image rather than the usual block-based approach commonly found in image and video compression schemes, the transform does not allow for local spatial control of the watermark insertion process. In other words, the addition of a watermark value to one DCT coefficient affects the entire image. The method in M. Barni *et el*. [16] is a slight modification of previous work [14], where the authors allow the user to determine the scaling factor and coefficients to be marked. The user-defined scaling factor and watermark length will greatly influence the effectiveness of this scheme both in terms of transparency and robustness. In all [14, 15, 16], original image is required for watermark extraction.

In [17], S. Burgett *et el.* uses block based DCT approach to embed the watermark. The image is segmented into 8×8 non-overlapping blocks and the DCT of each block is obtained similar to JPEG. A random subset of the blocks is chosen and a triplet of midrange frequency coefficients is slightly altered to encode a binary sequence. This seems to be a reasonable approach for adding some sort of perceptual criterion. Watermarks inserted into the high frequencies are most vulnerable to attack, whereas the low-frequency components are perceptually significant and very sensitive to alterations; such alterations may make the

watermark visible. Bors and Pitas [18] suggest a method that modifies DCT coefficients satisfying a block site selection constraint. The image is first divided into blocks of size 8×8. Certain blocks are then selected according to a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region, to convey the watermark information. In [17, 18], original image is not required for watermark extraction. This technique provides reasonable results on average, although a more image-dependent scheme could provide better quality and robustness. Image adaptive watermarking scheme using HVS model improves the performance of the watermarking techniques.

Swanson *et al*. [19] suggest a DCT domain watermarking technique, based on frequency masking of DCT blocks. The input image is split up into square blocks for which the DCT is computed. For each DCT block, a frequency mask is computed based on the knowledge that a masking grating raises the visual threshold for signal gratings around the masking frequency. The resulting perceptual mask is scaled and multiplied by the DCT of a maximal length PN sequence. This watermark is then added to the corresponding DCT block followed by spatial masking to verify that the watermark is invisible and to control the scaling factor. Watermark detection requires the original image as well as the original watermark and is accomplished by hypothesis testing. The scheme is robust against JPEG compression, noise, and cropping.

Tao and Dickinson [20] propose an adaptive block based DCT domain watermarking technique based on a regional perceptual classifier with assigned sensitivity indexes. The watermark is embedded in N AC DCT coefficients. The coefficients are selected as to have the smallest quantization step sizes according to the default JPEG compression table. Various approaches exist to determine the noise sensitivity by efficiently exploiting the masking effects of the HVS. The authors propose a regional classification algorithm which classifies the block in one of six perceptual classes. The classification algorithm exploits luminance masking, edge masking, and texture masking effects of the HVS. Namely the perceptual block classes from one to six are defined as: edge; uniform; low sensitivity; moderately busy; busy; and very busy, in descending order of noise sensitivity. Each perceptual class has a noise-sensitivity index assigned to it. Watermark recovery requires the original image as well as the watermark and is based on hypothesis testing. The author report shows that the method is robust to JPEG compression and additive noise.

C. Podilchuk, and W. Zeng [21] propose a watermarking technique for digital images that is based on utilizing visual models, which have been developed in the context of image compression. The visual model gives a direct way to determine the maximum amount of watermark signal that each portion of an image can tolerate without affecting the visual quality of the image. The watermark encoding scheme consists of a frequency decomposition based on a 8×8 framework followed by just noticeable difference (JND) calculation and watermark insertion. The watermark scheme is robust to different attacks such as JPEG compression, additive noise, scaling etc.

J. Wu, and J. Xie [22] propose an adaptive watermarking technique in DCT domain using HVS model and fuzzy c-means technique (FCM). In this method FCM technique is used to classify non-overlapping 8×8 original blocks into categories: one is suitable for watermarking with high imperceptibility and robustness and the other is unsuitable. Watermark is inserted in DCT mid-frequency coefficients of selected blocks. W. Zhang *et el.* [23] propose an adaptive digital watermarking approach. In this method FCM technique is used to determine the watermark strength of each image pixel, and then watermark is inserted adaptively to the N largest magnitude non-dc DCT coefficients of the host image. The both the method performs better against additive noise, compression and cropping etc.

Yifei Pu. *et el.* [24] proposes a public adaptive watermark algorithm for color images based on principal components analysis of generalized Hebb. The algorithm is based on principal component analysis of generalized Hebb adaptive algorithm in Artificial Neural Network and to do adaptive quantitative coding for principal component coefficients according to the proportion of marginal or textural information of the watermark image. In addition, it adaptively adjusts the embedding depth according to the images features to ensure the invisibility of the watermark. By way of disporting and stochastic embedding into color image watermark, it increases the embedding robusticity of watermark.

Although embedding watermark in host image by DCT is more robust than that of by DFT, the DWT has a number of advantages over the DCT, because the DWT provides both space and frequency localization, and different resolution levels. Thus, DWT based watermarking algorithm can effectively utilize the characteristics of HVS (Human Visual System) to attain good trade-off between robustness and imperceptibility. So, DWT based watermarking algorithms have gained more interest among the watermark researchers.

X.-G. Xia *et el.* [25] proposes a multiresolution watermark for digital images. The technique is implemented in DWT domain and watermark is inserted in the same way as described in method [15]. C. Podilchuk, and W. Zeng [26] propose image adaptive watermarking using visual models. The method is implemented using DWT and a HVS model and watermark is embedded adaptively by calculating just noticeable difference (JND) for each block regions. M.-S. Hseih [27] proposes a hiding digital watermarks using multiresolution wavelet transform. In this method original image is decomposed into wavelet coefficients. The method embeds a visually recognizable binary or gray image by modifying the mid frequency part of the image. Watermarking methods is based on the qualified significant wavelet tree which comes from the concept of embedded zero wavelet tree (EZW). The above methods are robust to a variety of signal distortions and requires original image for watermark extraction. In methods [25, 26, 27] the watermark embedded linearly to the original image. Deepa Kundur, and D. Hatzinakos [28] propose a digital watermarking using multiresolution wavelet decomposition. In this method watermark is embedded non-linearly in the original image by using scalar quantization, and image fusion principle concept. Original image is not required for watermark extraction. In this thesis we propose a fusion based image adaptive watermarking method using wavelet transform and a HVS model based on contrast sensitivity.

In [29] Mauro Barni *et el.* have proposed a scheme where in contrast to conventional methods operating in the wavelet domain, masking is accomplished pixel by pixel by taking into account the texture and the luminance content of all the image sub-bands. The watermark consists of a pseudorandom sequence which is adaptively added to the largest detain bands. As usual, the watermark is detected by computing the correlation between the watermarked coefficients and watermarking code, anyway detection threshold is chosen in such way that the knowledge of watermark energy used in the embedding phase is not needed, thus permitting to adapt it to the image at hand.

In [30] Xiangui Kang *et el.* have proposed a blind discrete wavelet transform- discrete Fourier transform (DWT-DFT) composite image watermarking algorithm that is robust against both affine transform and JPEG compression. This algorithm improves the robustness via using new embedding strategies, watermark structure, 2-D interleaving, and synchronization technique. A spread spectrum based informative watermark with a training sequence are embedded in the coefficients of the LL sub-band in the DWT domain while a template is embedded in the middle frequency components in the DFT domain. In watermark extraction, we first detect the template

in a possibly corrupted watermarked image to obtain the parameters of affine transform and convert the image back to its original shape. Then we perform translation registration by using the training sequence embedded in the DWT domain and finally extract the informative watermark.

In [31] Jianzhen wu *et el.* have proposed a blind wavelet based watermarking scheme using fuzzy clustering theory. The watermarking scheme utilizes the HVS by clustering the local image features, and thus can embed more robust watermark under a certain visual distance. Watermark bits are embedded through a PN sequence. In order to improve the robustness, we embed watermark several times in different position, which are randomly chosen. Similarly, in this thesis we propose a spread spectrum based blind image adaptive watermarking method using wavelet transform and a HVS model based on contrast sensitivity.

In [32] Zhang Guannan *et el.* have proposed an adaptive block-based blind watermarking algorithm using DWT. By analyzing the characteristic of detail sub-band coefficients of the image after discrete wavelet transform, we use the mean and variance of the detail sub-bands to modify the wavelet coefficients adaptively to embed the watermark**.** This is a blind watermark algorithm to confirm the copyright without the original image and the watermark is a meaningful binary image. The author report concludes that the algorithm is robust to common image processing operations.

2.5 CHAPTER SUMMARY

The various watermarking attacks in the image processing domain were discussed. Parameters that measure the performance of watermarking algorithms against different attacks were presented. The existing watermarking algorithms in different domain found in academic literature are also surveyed.

CHAPTER 3

FUSION-BASED WATERMARKING

Introduction

Algorithm Description

Simulation Results and Discussion

Chapter Summary

3.1 INTRODUCTION

This chapter presents an approach for robust source extraction watermarking algorithm based on multi-resolution image fusion principle. We address the problem of embedding binary images, gray images robustly within the host signal. The method transforms both the host image and watermark into the discrete wavelet domain where their coefficients are fused according to a series combination rule that take into account contrast sensitivity characteristics of the HVS [36]. The watermark is restricted to be much smaller in dimension than the host signal. No randomly generated keys are required for security, but the host image is necessary for watermark extraction. The method repeatedly merges the watermark coefficients at the various resolution levels of the host signal which provides simultaneous spatial localization and frequency spread of the watermark to provide robustness against widely varying signal distortions including cropping and filtering. The watermarking process is adaptive and depends on the local host image characteristics at each resolution level. Moreover, the watermark is resilient to attack since it is embedded strongly in more salient components of the image.

We develop our approach to fulfill the following requirements of a successful robust watermarking scheme:

1. The data hiding technique is adaptive and takes into account the natural masking characteristics of the host signal to more strongly, and hence, reliably embed the watermark.
2. The embedded watermark is robust to a reasonable level of signal distortion. Since the host signal is available for watermark extraction, it is exploited to characterize any attacks.
3. The algorithm is portable to different applications and can hide different types of information robustly within a host signal.

Research into human perceptions indicates that the retina of the eye splits an image into several components which circulates from the eye to the cortex in differently tuned channels (frequency bands). These channels can only be excited by the component of a signal with similar characteristics. The processing of signals in different channels is independent. Studies have shown that each of these channels have a bandwidth of approximately one octave [33]. Similarly, in a multi-resolution decomposition, the image is separated into bands of approximately equal

bandwidth on a logarithmic scale. It is therefore expected that use of the discrete wavelet transform will allow the independent processing of the resulting components without significant perceptible interaction with them.

For this reason, wavelet decomposition is attractive for the fusion of images. Image fusion refers to the processing and synergistic combinations of images from various knowledge sources and sensors to provide an overall result which contains the most relevant characteristics of its components. Since the process of image fusion is essentially a sensor-compressed information problem (i.e., it involves the combining of one or more images into a single fused result), it follows that wavelets are also useful for such merging.

Some multi-resolution wavelet fusion methods make use of information about the HVS to determine the perceptually most significant information from each image to retain the composite [34]. It is then expected that such rules can be used to judiciously select the regions of the host image in which to embed the watermark.

3.2 ALGORITHM DESCRIPTION

Throughout our discussion, we use $X(m,n)$ to denote the host image and $w(m,n)$ the watermark. The watermark, assumed to be a two dimensional array of real elements. The watermark is visually recognizable binary or gray scale image. The size of the watermark is $N \times N$. It is required that the size of the watermark in relation to the host image be "small". We assume, without loss of generality, that the watermark is smaller than the host by a factor of 2^M, where M is an integer greater or equal to 1.

3.2.1 Watermark Embedding Method

The technique is comprised of the 3 main stages is summarized in Figure 3.1. First, the image and watermark both are decomposed using the DWT. In the second stage, the watermark is selectively and repeatedly merged using a model of human contrast sensitivity to determine the most salient localized host image components. Last, the inverse DWT is applied to form the watermarked image. The following is the more detailed and analytic description of the procedure.

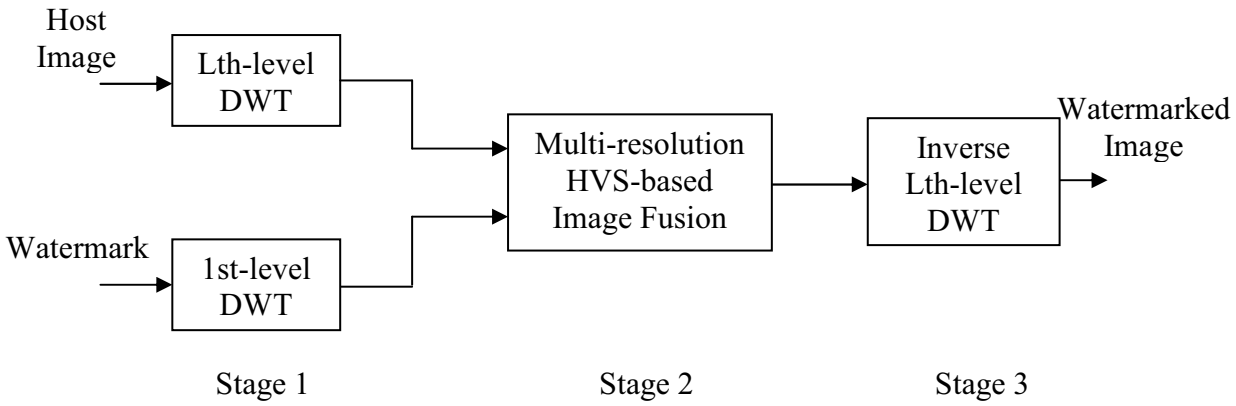


Figure 3.1: The Fusion-Based Watermark Embedding Method

Stage 1:

The host image and the watermark are transformed into the wavelet domain. We perform the L^{th} level DWT of the host image to produce a sequence of $3L$ detail images, corresponding to the horizontal, vertical, diagonal details at each resolution levels, and a gross approximation image at the coarsest resolution level. The value of L is equal to $M+1$. We denote the k^{th} detail image component at the l^{th} resolution level of the host by $X_{k,l}(m,n)$, where $k=1,2,3$ represents the frequency orientation corresponding to the horizontal, vertical and diagonal image details, $l=1,....,L$ the resolution level and (m,n) particular pair spatial location index at the resolution l .The gross approximation is represented by $X_{4,L}(m,n)$ where the subscript "4" is used instead of k to denote the gross image approximation at resolution L .

Similarly, the first level DWT of the watermark w is performed to produce $N_{wx} \times N_{wy}$ dimensional detail and approximation sub-images denoted by $w_{k,1}(m,n)$ where $k=1,2,3,4$.

Stage 2:

The each sub-images of the host are segmented into non-overlapping $N_{wx} \times N_{wy}$ blocks. Figure 3.2 demonstrates the procedure. We denote the segments by $X^{i}_{k,l}(m,n)$ where $i=1,2,....,2^{2(M+1-l)}$ is the total number of blocks at each frequency orientation k and resolution l .

The salience, S (which is numerical measure of perceptual importance) of each of the localized blocks is computed using information about the HVS model based on contrast sensitivity. The value of the salience determines the strength of the watermark to embed in the particular $N_{wx} \times N_{wy}$ coefficient image block. To define our measure of salience, we first introduce the notion of contrast sensitivity. Mathematically contrast sensitivity is defined as the

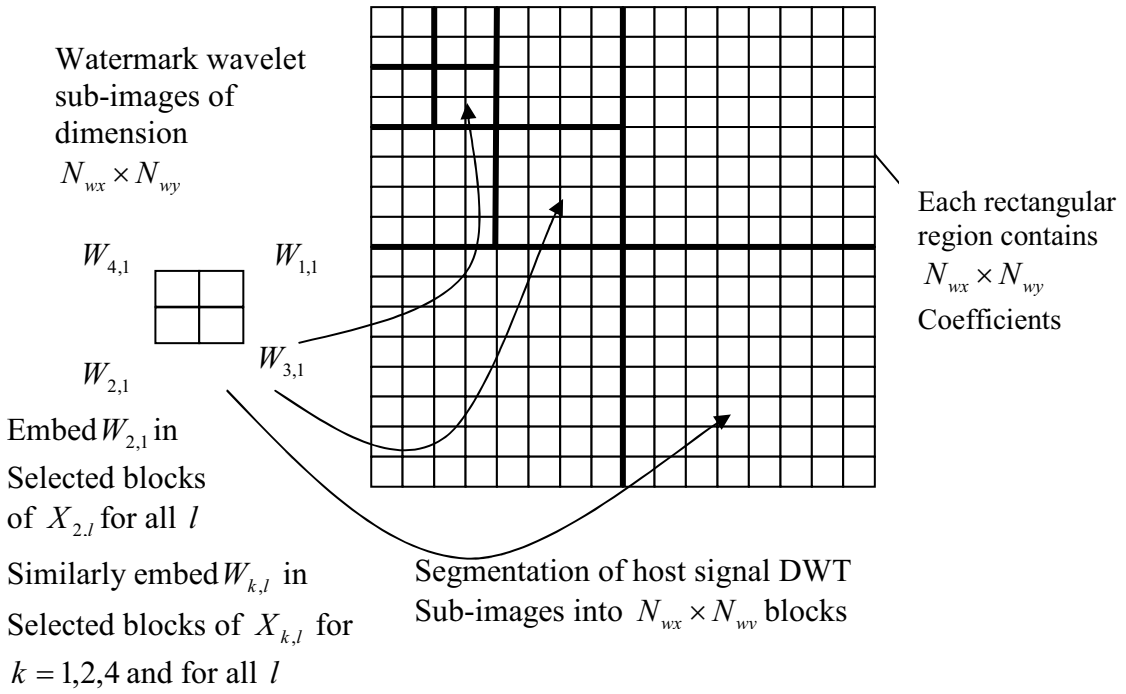


Figure 3.2: Segmentation of the Host Image Wavelet Coefficients into $N_{wx} \times N_{wy}$ Blocks for Fusion Watermarking. The Salience of each block is computed and if it is above a specified threshold, the corresponding $N_{wx} \times N_{wy}$ watermark wavelet coefficient is embedded. As suggested by the diagram, the watermark is more widely spread spatially when embedded at a lower (coarser) resolution

reciprocal of the contrast necessary for a given spatial frequency to be perceived. For this paper we assume the well known model given by Dooley [35]. We extend the model to two dimensional using the same approach as [34]. The resulting contrast sensitivity for a particular pair of spatial frequency is given by:

$$C(u,v) = 5.05e^{-0.178(u+v)}(e^{0.1(u+v)} - 1) \qquad 3.1$$

Where $C(u,v)$ is the contrast sensitivity matrix and u, and v are the spatial frequencies. The salience of each block is defined as:

$$S(X^i_{k,l}(m,n)) = \sum_{\forall(u,v)} C(u,v)\left|F^i_{k,l}(u,v)\right|^2 \qquad 3.2$$

Where $F^i_{k,l}(u,v)$ the normalized discrete Fourier is transform of the image component $X^i_{k,l}(m,n)$; $F^i_{k,l}(u,v)$ is normalized such that it has unit energy (i.e. $\left\|F^i_{k,l}(u,v)\right\|^2 = 1$). The image fusion method presented relies on the contrast sensitivity of the HVS to determine the importance of the information.

The watermark is embedded only in *B* percent of the most salient detail image blocks at each resolution level and orientation using the following equation:

$$X_{k,l}^{w,i}(m,n) = X_{k,l}^{i}(m,n) + \alpha_{k,l}^{i}\sqrt{\frac{S(X_{k,l}^{i}(m,n))}{\max S(X_{k,l}^{i}(m,n))}}w_{k,l}(m,n) \qquad 3.3$$

where $X_{k,l}^{w,i}(m,n)$ are the watermarked DWT coefficients. For the remaining blocks, we set

$$X_{k,l}^{w,i}(m,n) = X_{k,l}^{i}(m,n) \qquad 3.4$$

where $\alpha_{k,l}^{i}$ are positive real numbers that determine a tradeoff between the imperceptibility and robustness against attacks at each of the resolution levels. The value of $\alpha_{k,l}^{i}$ is adaptively changed according to the resolution level. The value of $\alpha_{k,l}^{i}$ ranges between 5% and 75% of the mean value of the detail image blocks. For each resolution levels, the value of $\alpha_{k,l}^{i}$ is set such that lower value for higher resolution level and correspondingly higher value for next lower resolution levels. The fraction within the square root is a relative measure that gives greater weight judiciously to the embedded watermark in more salient host image regions.

A similar merging procedure is used to embed the watermark approximation coefficients $w_{4,1}(m,n)$ into the host image approximation block $X_{4,L}^{i}(m,n)$. The watermark is embedded in all blocks. The value of $\alpha_{4,L}$ is set between 1% and 5% of the mean value of the approximate image block to ensure imperceptibility.

The larger the magnitude of $\alpha_{k,l}$, the more robust and visible the watermark; the ranges of value suggested provide an appropriate trade-off for most photographic images. Similarly, the larger the value of *B,* the greater the number of coefficient blocks in which the watermark is embedded at each resolution level which also comes at the expense of increased visibility; simulation results shows that a range of *B* between 25 and 75 allows for appropriate marking.

Stage 3:

The corresponding L^{th} level inverse DWT (IDWT) of the fused image components $X_{k,l}^{w}(m,n)$ is computed to form the watermarked image.

3.2.2 Watermark Extracting Method

The objective of the extraction process is to reliably obtain an estimate of the original watermark from a possibly distortion version of the watermarked image X_w. The reconstruction process

requires knowledge of the original host image X. The watermark is extracted from the possibly corrupted watermarked image using the host image, by applying the inverse procedure at each resolution level to obtain an estimate of the watermark. The estimates for each resolution level are averaged to produce an overall estimate of the watermark. The normalized correlation coefficient r was used to measure the robustness of the extracted watermark against different attacks.

3.3 SIMULATION RESULTS AND DISCUSSION

For simulations, we take Lena image of size 512×512 as the host image shown in Fig. 3.3(a) and watermark is visually recognizable gray-scale image of size 32×32 shown in Fig. 3.3(b). To form the watermark, the DC value is first subtracted from the watermark image and then made its variance value to 1, before watermark image is used for simulation. We chose $B = 75$, $L = 5$; and α value was set to 60, 40, 20, 10, and 5 percent of mean value of detail image blocks for lower resolution level to higher resolution level respectively, and α value was set to 1.6% of approximate image blocks in our simulation. The PSNR value of watermarked image is 37.5381 as shown in Fig. 3.3(c), and is perceptually identical to the original host and watermark can be exactly extracted. The resulting watermarked image is corrupted using one of many common distortions which we discuss in the subsequent section. When the watermark was extracted it was scaled, so that its minimum pixel value was set to black and its maximum pixel value to white and correlated with the embedded watermark to measure the robustness and detection capability of the technique

Robustness against JPEG Lossy Compression

Figure 2(a) shows the effect of compression on the correlation coefficient for different quality factors. The correlation coefficient remains high for reasonable quality factor values. Severe visual image degradation in which the features of the face were not distinguishable occurred for quality factors of 15 and above. The results show that the watermark still remains present and correlation coefficient is still high about 0.8. Fig. 3.4(b), and 3.4(d) shows the degraded watermarked image and Fig. 3.4(c) and 3.4(e) shows the corresponding extracted watermark for quality factor 15 and 5 respectively.

Robustness against AWGN Noise

Figure 3.5(a) provides the results for degradation using additive white Gaussian noise. The proposed method performs well in the presence of additive noise. Severe visual image degradation occurred at signal to noise ratios of 15 dB and greater. Although the image appeared overwhelmed by noise, the watermark can be detected with a correlation of about 0.8. Fig. 3.5(b), and 3.5(d) shows the degraded watermarked image and Fig. 3.5(c), and 3.5(e) shows the corresponding extracted watermark for SNR 15dB and 10dB respectively.

Robustness against Filtering

The results for degradations from median and mean filtering are also presented in Fig. 3.6(a) and 3.7(a) respectively. The watermarked image was filtered with a $F \times F$ mean (or median) filter. Highly noticeable image degradation began to occur for $F > 9$. The watermark can still be detected. . Fig. 3.6(b), and 3.6(d) shows the degraded watermarked image and 3.6(c), and 3.6(e) shows the corresponding extracted watermark for median filtering of order 5×5 and 9×9 respectively. Fig. 3.7(b), and 3.7(d) shows the degraded watermarked image and 3.7(c), and 3.7(e) shows the corresponding extracted watermark for mean filtering of order 5×5 and 9×9 respectively.

Robustness against Cropping

Fig 3.8(a) shows the effect of image cropping on watermark extraction. For watermark extraction, the portion of the watermarked image cropped out was replaced with the host image. Even when only 25% of the image area cropped, the correlation value for the proposed technique is high about 0.9. Fig. 3.8(b), and 3.8(d) shows the degraded watermarked image and Fig. 3.8(c) and 3.8(e) shows the extracted watermark for 12.5% and 25% image area cropped respectively.

Robustness against Image Resizing

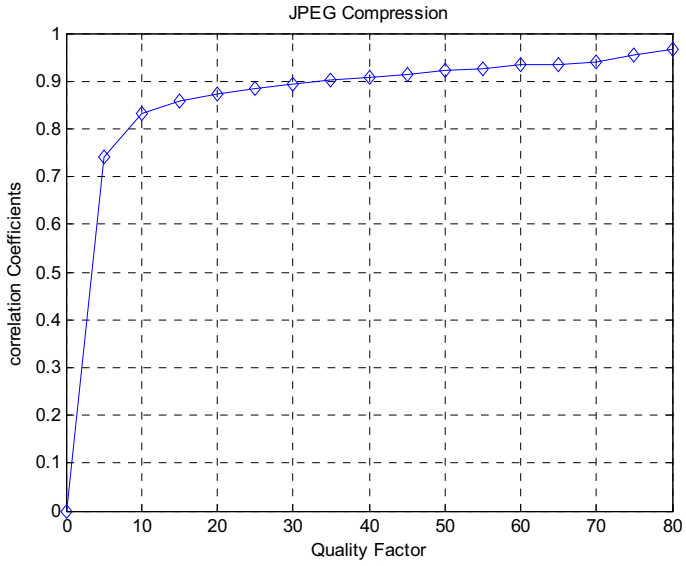
Fig 3.9(a) shows the results of the watermarked images. The images were scaled down in size by a factor of F using bilinear interpolation and were resized to their original dimension before watermark extraction. Visible degradation occurs for high value of F due to resolution adjustment, but the watermark can still be detected with correlation of about 0.8. Fig. 3.9(b), and 3.9(d) shows the degraded watermarked image and Fig. 3.9(c) and 3.9(e) shows the extracted watermark for image scaling down by a factor of 5 and 7 respectively.

(a)

(b)

(c)

Fig.3.3. Results for Fusion-Based Watermarking Method Without any Attack: (a) original image, (b) watermark image, (c) watermarked image.



(a)

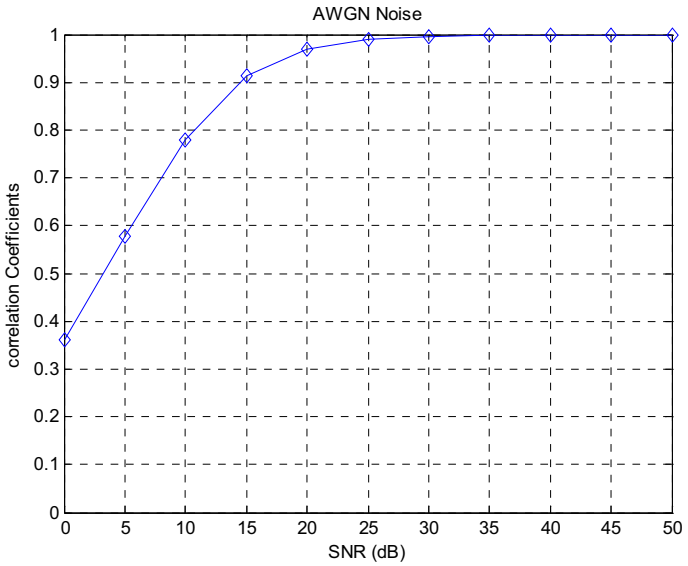
(b)

(c)

(d)

(e)

Fig.3.4 Results for JPEG Compression, (a)Correlation coefficient vs. Quality factor (QF), (b) degraded watermarked image for QF=15, (c) extracted watermark for QF=15, (d) degraded watermarked image for QF =5, (e) extracted watermark for QF=5.

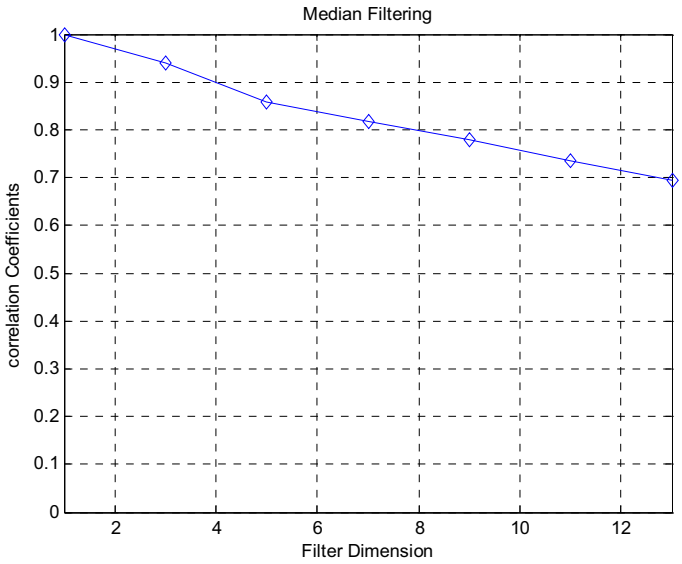


.

(b) (c)

(d) (e)

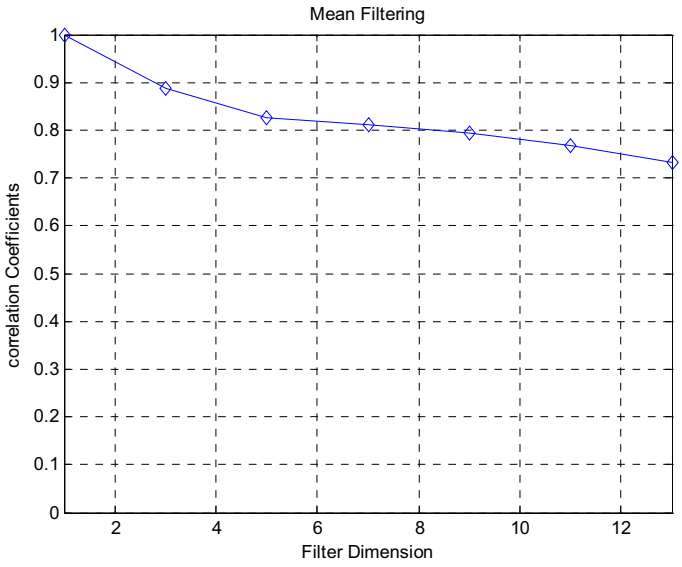
Fig.3.5 Results for Additive White Gaussian Noise Degradation, (a)Correlation coefficient vs. SNR, (b) degraded watermarked image for SNR=15dB, (c) extracted watermark for SNR=15dB, (d) degraded watermarked image for SNR=10dB, (e) extracted watermark for SNR=10dB.



(b) (c)

(d) (e)

Fig.3.6 Results for Median Filtering, (a)Correlation coefficient vs. dimension of filter *F*, (b) degraded watermarked image for *F*=5, (c) extracted watermark for *F*=5, (d) degraded watermarked image for *F* =9, (e) extracted watermark for *F*=9.



(a)

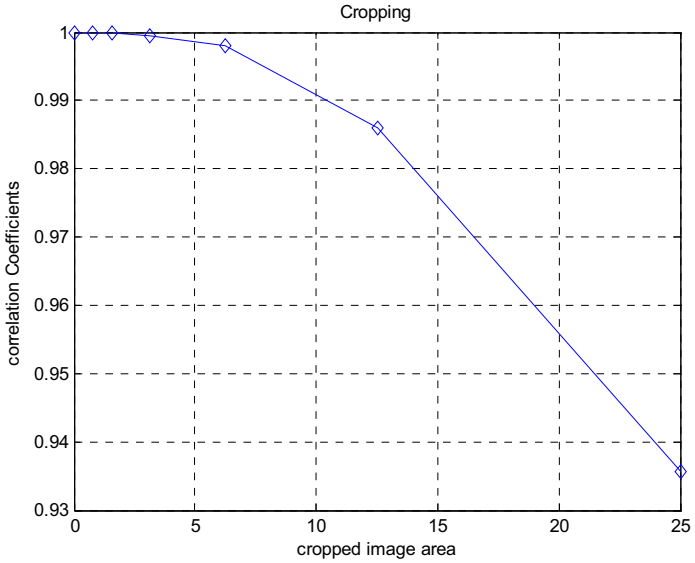
(b)

(c)

(d)

(e)

Fig.3.7 Results for Mean Filtering, (a)Correlation coefficient vs. dimension of filter *F*, (b) degraded watermarked image for *F*=5, (c) extracted watermark for *F*=5, (d) degraded watermarked image for *F* =9, (e) extracted watermark for *F*=9.



(a)

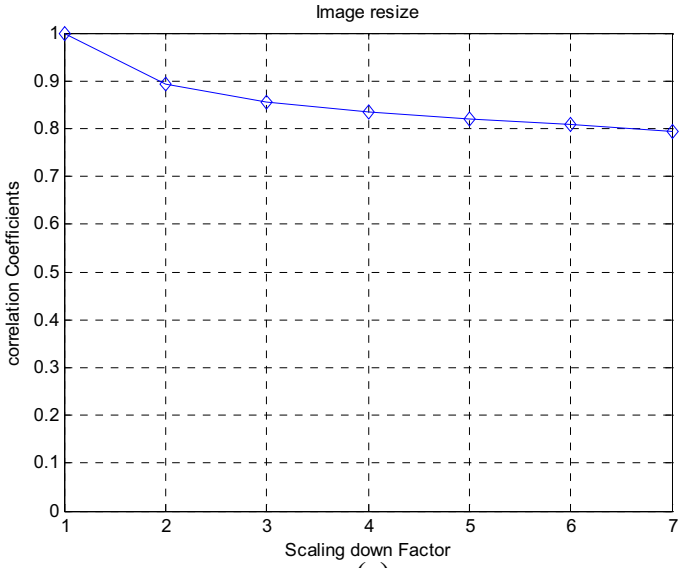
(b)

(c)

(d)

(e)

Fig.3.8 Results for Cropping, (a) Correlation coefficient vs. percent cropped image area, (b) degraded watermarked image for 12.5% image area cropped, (c) extracted watermark for 12.5% image area cropped, (d) degraded watermarked image for 25% image area cropped, (e) extracted watermark for 25% image area cropped.



(a)

(b) (c)

(d) (e)

Fig.3.9 Results for Image Resizing, (a) Correlation coefficient vs. image scaling down factor, (b) degraded watermarked image for factor 5, (c) extracted watermark for factor 7, (d) degraded watermarked image for factor 5, (e) extracted watermark for factor 7.

A simulation result shows that, the multiresolution fusion-based watermarking method performs better against different attacks. The use of the DWT domain inherently makes our design more resilient to localized spatial and frequency domain distortions including filtering, resolution reduction and cropping. From experience with other host images, we find that the method works significantly better for images with highly varying localized characteristics) i.e., images with both smooth and busy areas). This is due to the fact that our HVS-based merging rule adapts the watermark signal strength to the local masking characteristics of the host image. Thus, a higher energy signal can be imperceptibly embedded with in all regions of the signal. An advantage of our method is its flexibility in embedding both binary and grayscale logo watermarks. Experimentally, we found that the embedded watermark undergoes at worst the same level of perceptible distortion as the watermarked image. This is an inherent advantage to our fusion-based watermarking scheme since an attacker would have to destroy the watermarked image to guarantee that the watermark was sufficiently degraded.

3.4 CHAPTER SUMMARY

A multiresolution fusion based watermarking technique employing a model of the HVS was described in the chapter. The key features of the approach are summarized below:

- The watermark is first decomposed using a 1^{st}-level DWT so that its detail coefficients can be repeatedly embedded into the corresponding detail coefficients of the host using a model of HVS. This process involves merging components of the watermark with similar characteristics within those of the host image, so that the technique better exploits the masking properties of the host signal. Hence watermark is embedded with much stronger energy while remaining imperceptible within the host signal.
- The technique embeds the watermark DWT coefficients repeatedly in the discrete wavelet domain which inherently makes the watermark more resilient to filtering, cropping, and resolution reduction than techniques using other type of transforms.

CHAPTER 4

SPREAD SPECTRUM-BASED WATERMARKING

Introduction

Algorithm Description

Simulation Results and Discussion

Chapter Summary

4.1 INTRODUCTION

This chapter presents an approach for robust destination extraction watermarking based on spread spectrum principle. We address the problem of embedding binary data, and visually recognizable binary images robustly within the host signal. The method transforms the host signal into the discrete wavelet domain where the watermark bits are embedded through a pseudo-random white noise sequence in the middle frequency sub-bands to achieve good tradeoff between robustness and imperceptibility [31]. The watermark bits are adaptively embedded in the host signal by utilizing the contrast sensitivity characteristics of the human visual system (HVS). No original image is required for watermark extraction, but only a secret key is necessary for extraction. Hence watermarking process is more practical. The watermarking process is adaptive and depends on the local host image characteristics. Moreover, the watermark is resilient to attack since watermark bit is embedded strongly in more salient components of the image. The main advantages of the proposed watermarking method are listed below:

1. The data hiding technique is adaptive and takes into account the natural masking characteristics of the host signal to more strongly, and hence, reliably embed the watermark.
2. The data hiding technique is more practical as no original image is required for watermark extraction.
3. The visually recognizable binary image can be used as watermark to claim one's ownership.

4.2 ALGORITHM DESCRIPTION

In the proposed watermarking scheme, we use $X(m,n)$ to denote the host image and visually recognizable binary image $w(m,n)$ is used as watermark.

4.2.1 Watermark Embedding Method:

The watermark embedding technique is comprised of the 3 main stage discussed below. First, the image is decomposed using the DWT. In the second stage, the watermark bits are adaptively embedded through a PN-sequence using a model of human contrast sensitivity. Last, the inverse DWT is applied to form the watermarked image. The following is the more detailed and analytic description of the procedure.

Stage 1:

The host image is transformed into the wavelet domain. We perform the 1st-level discrete wavelet decomposition of the original image, and we got 3 detail images, corresponding to the horizontal, vertical, diagonal details, and 1 gross approximation image. We denote the k^{th} detail image component of the host by $X_{k,1}(m,n)$, where $k = 1,2,3$ represents the frequency orientation corresponding to the horizontal, vertical and diagonal image details, and 1 represents the first resolution level and (m,n) particular pair spatial location index. The gross approximation is represented by $X_{4,1}(m,n)$ where the subscript "4" is used instead of k to denote the gross approximation image. In order to avoid serious image degradation and survive lossy compression, we will embed the watermark in the middle frequency band that is $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$. We split $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band into non-overlapping 8×8 blocks respectively, suppose that the original image is of $M \times M$, then $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ will be of size $\frac{M}{2}\times\frac{M}{2}$. After splitting there will be $\frac{M}{16}\times\frac{M}{16}$ blocks respectively in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band.

The watermark image is converted into an array of bits. If the watermark is 32×32, the number of bits is 1024. The number of watermark bits used should be less than total number of blocks in $X_{1,1}(m,n)$ or $X_{2,1}(m,n)$ sub-band.

Stage 2:

The salience *S* (which is a numerical measure of perceptual importance) of each of these localized segments is computed using information about the contrast sensitivity characteristics of the HVS. The value of the salience determines the strength of the watermark to embed in the particular 8×8 coefficient image block. Mathematically, contrast sensitivity is defined as the reciprocal of the contrast necessary for a given spatial frequency to be perceived.

The salience *S* of each localized block is determined by the same procedure as described in chapter 3. Again for convenience the resulting contrast sensitivity for a particular pair of spatial frequencies is given by:

$$C(u,v) = 5.05e^{-0.178(u+v)}(e^{0.1(u+v)} - 1) \qquad 4.1$$

where $C(u,v)$ is the contrast sensitivity matrix and u and v are the spatial frequencies. The salience of each block is defined as:

$$S(X^i_{k,1}(m,n)) = \sum_{\forall(u,v)} C(u,v)\left|F_{k,1}(u,v)\right|^2 \qquad 4.2$$

where $F^i_{k,l}(u,v)$ the normalized discrete Fourier is transform of the image component $X^i_{k,1}(m,n)$; $F^i_{k,1}(u,v)$ is normalized such that it has unit energy (i.e. $\left\|F^i_{k,1}(u,v)\right\|^2 = 1$). The method presented relies on the contrast sensitivity of the HVS to determine the importance of the information

In order to keep secret of watermark embedding position, we generate pseudo random number to be used as the allocation of the watermarking position of the blocks in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band. In generating the pseudo random number, a 'key' is used as a seed number. To fit the random number to the number of blocks in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$, it is scaled to the block numbers in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band. Watermark is embedded in chosen blocks in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ only. We use another different key to generate an 8 **x** 8 random sequence having distribution of $N(0,1)$ to embed a watermark bit in each chosen block. The same watermark bit is embedded in the chosen blocks, which have the same location in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band. Watermark bit embedding procedure can be represented as follows:

$$\beta^i_{k,1} = \sqrt{\frac{S(X^i_{k,l}(m,n))}{\max S(X^i_{k,l}(m,n))}} \qquad 4.3$$

If *watermark bit=1*

$$X^{w,ci}_{k,l}(m,n) = X^{ci}_{k,l}(m,n) + \alpha^{ci}_{k,l}\beta^{ci}_{k,l}PN\_one(m,n) \qquad 4.4$$

else

$$X^{w,ci}_{k,l}(m,n) = X^{ci}_{k,l}(m,n) - \alpha^{ci}_{k,l}\beta^{ci}_{k,l}PN\_one(m,n) \qquad 4.5$$

Where $1 \le m,n \le 8$, and $k = 1,2$, represents $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band respectively, $X^{w,ci}_{k,1}$ and $X^{ci}_{k,1}(m,n)$ are watermarked and original DWT coefficients of chosen blocks, $\beta^i_{k,l}$ are a relative measure that gives greater weight judiciously to the embedded watermark in more salient blocks in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band, $\alpha^i_{k,1}$ are positive real numbers that

determine a tradeoff between the imperceptibility and robustness against signal distortion. The $\alpha_{k,1}^{i}$ range between 50% and 95% of the mean value of the sub-band blocks. PN_one is random sequence.

Stage 3:

Perform one-level IDWT to obtain watermarked image.

4.2.2 Watermark Extracting Method:

The extraction process of watermark is rather similar to the embedding process, first we compute DWT of the watermarked image and spilt $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band into non-overlapping 8 **x** 8 blocks and then use the same key to generate the same random number by which to find the watermark embedding position, and also use the same key to generate random sequence which have the distribution of $N(0,1)$. Then we compute the correlation between PN_one and the coefficients of selected block that embed the same watermark bit both in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-band and calculate the average correlation. Watermark bit value can be decided as follows:

If correlation > 0
Watermark bit =1
else
Watermark bit =0

Watermark extraction is oblivious (blind), with no reference to the original image and thus is more practical than non-oblivious one. The normalized correlation coefficient r was used to measure the robustness of the extracted watermark against different attacks.

4.3 SIMULATION RESULTS AND DISCUSSION

For simulations, we take Lena image of size 512×512 as the host image shown in Fig. 4.1(a) and watermark is visually recognizable binary image of size 32×32 shown in Fig. 4.1(b). By using harr wavelets, we decompose Lena image into four sub-bands and watermark are embedded in $X_{1,1}(m,n)$ and $X_{2,1}(m,n)$ sub-bands. We chose α =90% in our simulation. . The PSNR value of watermarked image is 37.5001 as shown in Fig. 4.1(c), and is perceptually identical to the original host and watermark can be exactly extracted. The amplified absolute difference between the watermarked image and host image is shown in Fig. 4.1(d). Because of

the adaptive and localized nature of the embedding routine the watermarks takes on characteristics similar to the host image itself. The use of DWT and HVS allows the design of an embedded signal which is more naturally masked by the host image itself. This permits the embedding of a higher energy, and thus, more robust watermark. The resulting watermarked image is corrupted using one of many common distortions which we discuss in the subsequent section. The watermark was extracted from the corrupted image and correlated with the embedded watermark to measure the robustness and detection capability of the technique.

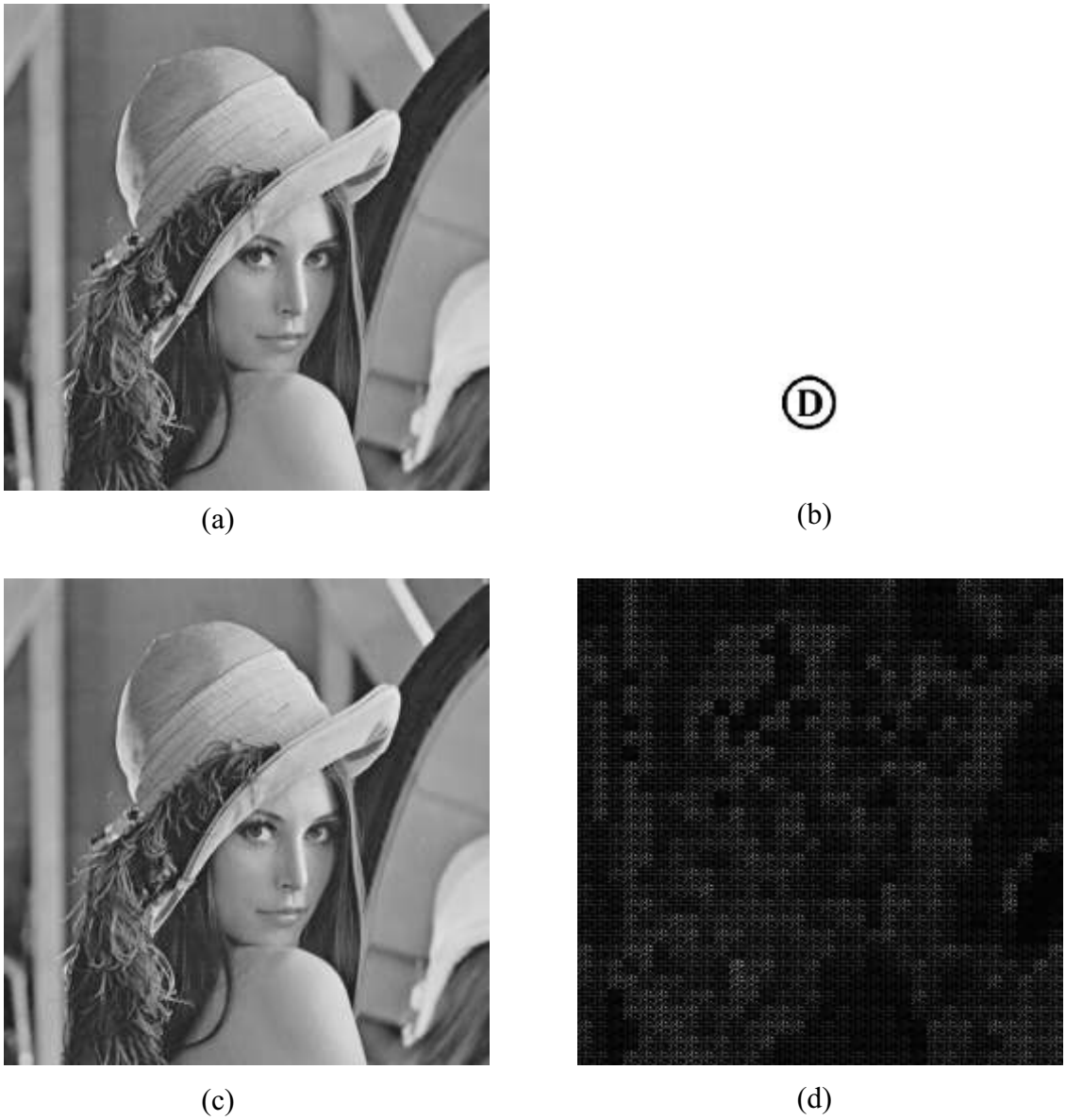
The result for JPEG compression is shown in Fig. 4.2(a) for varying quality factors (QF). Fig. 4.2 (b) and 4.2(d) shows the degraded watermarked image and Fig. 4.2 (c) and 4.2 (e) shows the corresponding extracted watermark for quality factor 40 and 25 respectively. The result shows that, the watermark is still present and visually detectable for quality factor of 20 and above.

Additive white Gaussian noise was added to the watermarked image to determine the robustness of the method to additive noise. Fig.4.3 (a) presents the result for varying SNRs. Fig. 4.3 (b), and 4.3 (d) shows the degraded watermarked image and Fig. 4.3 (c), and 4.3 (e) shows the corresponding extracted watermark for SNR 5dB and 15dB respectively. The result shows that, the watermark, however, had a high correlation for even high noise levels like 0dB.

The results for degradations from median filtering are also presented in Fig. 4.4(a). The watermarked image was filtered with a $F \times F$ median filter. Highly noticeable image degradation began to occur for $F > 5$. The watermark can still be detected. . Fig. 4.4 (b), and 4.4 (d) shows the degraded watermarked image and 4.4 (c), and 4.4 (e) shows the corresponding extracted watermark for median filtering of order 3×3 and 7×7 respectively. The results for Gaussian low pass filtering (rotationally symmetric blur) for different standard deviation (sigma) value are displayed in Fig. 4.5 (a). The watermark can still be detected for sigma value of above 1. Fig. 4.5 (b), and 4.5 (d) shows the degraded watermarked image and 4.5 (c), and 4.5 (e) shows the corresponding extracted watermark for Gaussian low pass filtering for sigma value of 1 and 2 respectively.

Fig 4.6(a) shows the effect of image cropping on watermark extraction. For watermark extraction, the portion of the watermarked image cropped out. Even when only 25% of the image area cropped, the correlation value for the proposed technique is high about 0.85. Fig. 4.6 (b),

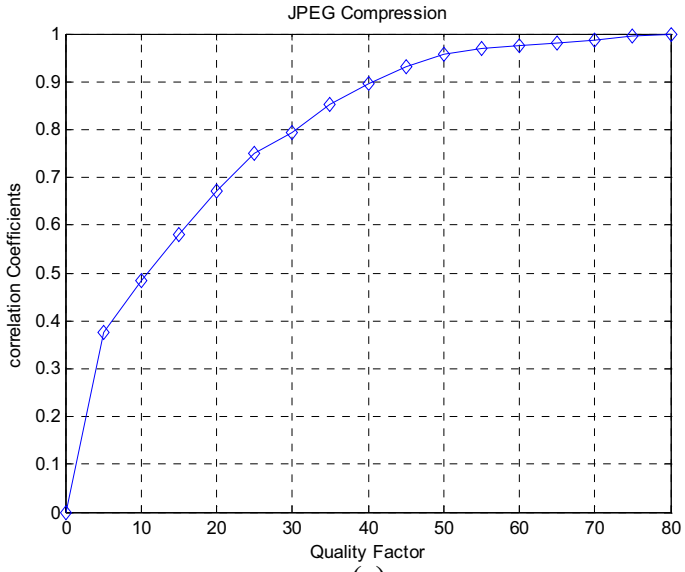
and 4.6 (d) shows the degraded watermarked image and Fig. 4.6 (c) and 4.6 (e) shows the extracted watermark for 12.5% and 25% image area cropped respectively.



(a) (b)

(c) (d)

Fig.4.1. Results for Spread Spectrum-Based Watermarking Method Without any Attack: (a) original image, (b) watermark image, (c) watermarked image, and (d) amplified absolute difference image.



(a)

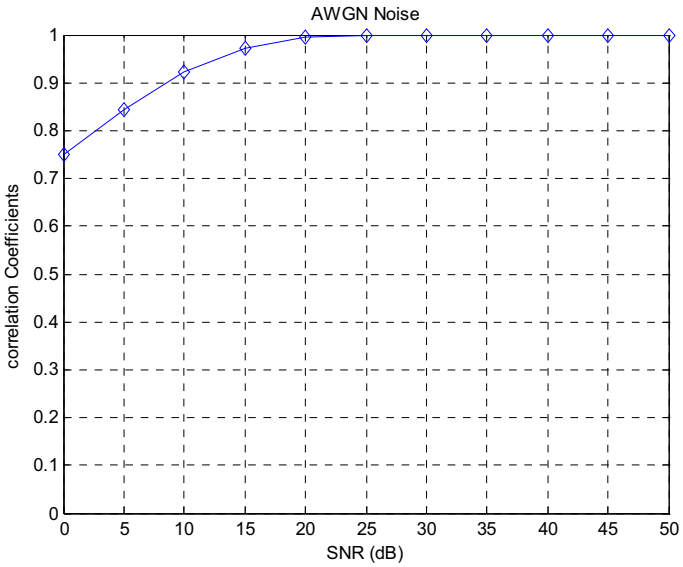
(b)

(c)

(d)

(e)

Fig. 4.2 Results for JPEG Compression, (a)Correlation coefficient vs. Quality factor (QF), (b) degraded watermarked image for QF=40, (c) extracted watermark for QF=40, (d) degraded watermarked image for QF =25, (e) extracted watermark for QF=25.



(a)

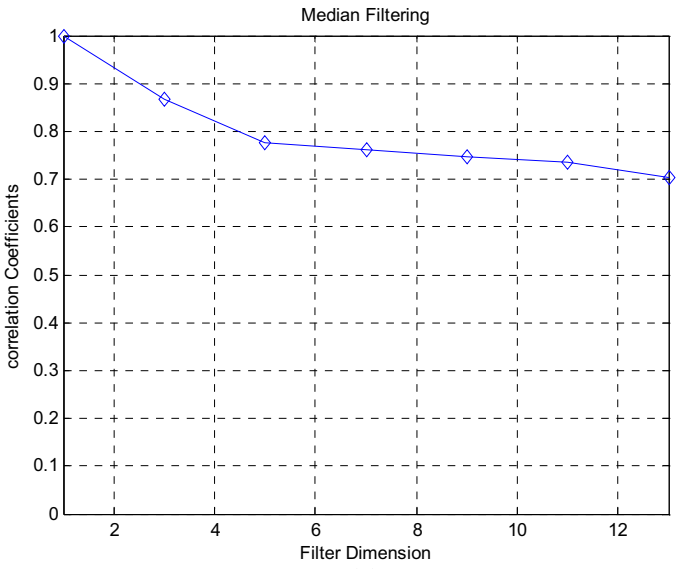
(b)

(c)

(d)

(e)

Fig.4.3 Results for Additive White Gaussian Noise Degradation, (a)Correlation coefficient vs. SNR, (b) degraded watermarked image for SNR=5dB, (c) extracted watermark for SNR=5dB, (d) degraded watermarked image for SNR=15dB, (e) extracted watermark for SNR=15dB.



(a)

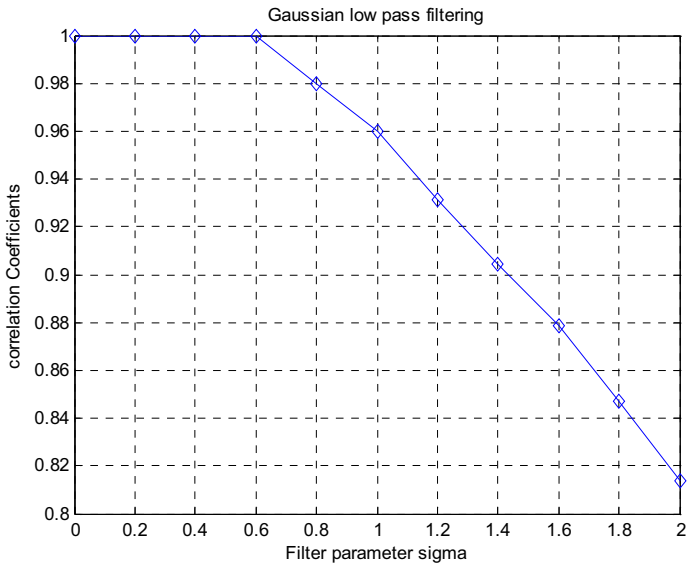
(b)

(c)

(d)

(e)

Fig.4.4 Results for Median Filtering, (a)Correlation coefficient vs. dimension of filter *F*, (b) degraded watermarked image for *F*=3, (c) extracted watermark for *F*=3, (d) degraded watermarked image for *F* =7, (e) extracted watermark for *F*=7.



(a)

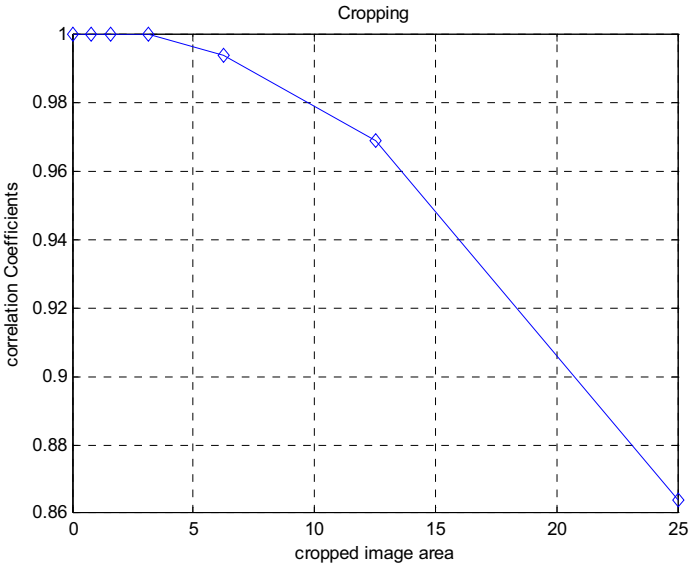
(b)

(c)

(d)

(e)

Fig.4.5 Results for Gaussian low pass Filtering, (a)Correlation coefficient vs. filter parameter sigma, (b) degraded watermarked image for sigma=1, (c) extracted watermark for sigma=1, (d) degraded watermarked image for sigma =2, (e) extracted watermark for sigma=2.



(a)

(b)

(c)

(d)

(e)

Fig.4.6 Results for Cropping, (a) Correlation coefficient vs. percent cropped image area, (b) degraded watermarked image for 12.5% image area cropped, (c) extracted watermark for 12.5% image area cropped, (d) degraded watermarked image for 25% image area cropped, (e) extracted watermark for 25% image area cropped.

The above described spread spectrum watermarking technique is a blind technique, i.e. host signal is not required for watermark extraction, hence the method is more practical. Simulation result shows that, the method performs better against attacks like AWGN noise, median and Gaussian low pass filtering, cropping, and JPEG compression but experimentally, we found that the method is not robust against mean filtering. From experience with other host images, we find that the method works significantly better for images with highly varying localized characteristics) i.e., images with both smooth and busy areas). This is due to the fact that our HVS-based merging rule adapts the watermark signal strength to the local masking characteristics of the host image. Thus, a higher energy signal can be imperceptibly embedded with in all regions of the signal.

4.4 CHAPTER SUMMARY:

A spread spectrum based watermarking technique employing a model of the HVS was described in the chapter. The key features of the approach are summarized below:

- The host image is first decomposed using a 1^{st}-level DWT. The watermark bits are adaptively embedded through a PN-sequence in the mid-frequency sub-bands using a HVS model to achieve good trade-off between robustness and imperceptibility.
- Watermark is extracted by judging the correlation value between original PN-sequence and coefficients of selected blocks where watermark is inserted in watermarked image. The method is more practical as no original image is required for watermark extraction.

CHAPTER 5

CONCLUSION

Conclusion

Future Work

5.1 CONCLUSION

The work in this thesis, primarily focus on to provide good tradeoff between perceptual quality of the watermarked image and its robustness to different attacks. For this purpose, we have discussed two digital watermarking algorithms in discrete wavelet domain (DWT) by incorporating contrast sensitivity based human visual system model (HVS). One is fusion based watermarking, and other is spread spectrum based watermarking. We used grayscale watermark for fusion based watermarking, and binary watermark for spread spectrum based watermarking. Through computer simulation, we analyzed the performance of the algorithms against different attacks such as JPEG compression, AWGN noise, mean and median filtering, cropping, and image resizing. The important points to conclude from the simulation analysis for fusion based watermarking algorithm were:

- Embedded watermark undergoes at worst the same level of perceptible distortion as the watermarked image.
- It is resilient to JPEG lossy compression up to quality factor 5. Severe visual image degradation occurred for quality factor of 15 and above, but still extracted watermark is visually recognizable and correlation coefficient is high about 0.8.
- It survives additive white Gaussian noise (AWGN) up to SNR of 10 dB.
- It is robust to both mean and median filtering up to filter order of 13. Highly Image degradation occurred for filter order of 9 and above, but still watermark is extractable with correlation coefficient value of about 0.75.
- It is very much robust to intentional attack cropping. Even though watermarked image is 25% cropped, the watermark is still extractable with correlation value of 0.93.
- It is immune to image resizing (scaling down).

For spread spectrum based watermarking, we concluded some of important points were:

- It is resilient to JPEG lossy compression up to quality factor 20.
- It is very much robust to AWGN noise. Even though watermarked image is degraded by 0 dB noise, the watermark is extractable with correlation value of about 0.75.
- It survives median filtering up to filter order 7, and Gaussian low pass filtering up to sigma value 2, but its performance is not acceptable for mean filtering.

- It is very much robust against intentional attack cropping.
- This method is more practical as no original image is required for watermark extraction.

From the simulation analysis, we conclude that the both the methods are robust against different non geometric attacks. However, both the methods fail for non-geometric attacks such as rotation or affine transformations.

5.2 FUTURE WORK

The discussed watermarking algorithms are robust to non-geometrics attacks only. We can extend this work by developing new watermarking algorithms, which are robust to both geometric attacks and non geometric attacks. Future work will also concentrate on making the watermarking methods more practical by modifying the techniques such that the host image is not required to extract the watermark and robust to both geometric and non geometric attacks.

REFERENCES

[1] Van Schyndel, R.G., Tirkel, A.Z., and Osborne, C.F., "A digital Watermark." Proc. of the IEEE Int. Conference on Image Processing. Vol. 2, (1994): pp. 86-90.

[2] Swanson, M.D., Kobayashi, M., and Tewfik, A.H., "Multimedia Data-Embedding and Watermarking Technologies." Proc. of the IEEE. Vol. 86, No. 6, (June 1998): pp. 1064–1087.

[3] Petitcolas, F., Anderson, R., and Kuhn, M., "Information Hiding - a Survey." Proc. of the IEEE. Vol. 87, No. 7, (July 1999): pp. 1062–1078.

[4] Barni, M., Bartolini, F., Cox, I.J., Hernandez, J., and Perez-Gonzalez, F., "Digital Watermarking for Copyright Protection: A communications perspective." IEEE Communications Magazine. Vol. 39, No. 8, (August 2001):pp. 90–133.

[5] Langelaar, Gerhard C., Setyawan, I., and Lagendijk, R.L., "Watermarking Digital Image and Video Data: A state-of-the-art-overview." IEEE Signal Processing Magazine. Vol. 17, No. 5, (September 2000): pp. 20-47.

[6] Voyatzis, G., Mikolaides, N., and Pitas, I., "Digital watermarking: An overview." Proc. of IX European Signal Processing Conference(EUSIPCO), Island of Rhodes, Greece. (September 8-11, 1998): pp. 13-16.

[7] Wolfgang, R.B., Podilchuk, C.I., and Edward J. Delp, "Perceptual Watermarks for Image and Video." Proc. of the IEEE. Vol. 87, No. 7, (July 1998): pp. 1109-1126.

[8] Cox, I.J., Miller, M.L., and Bloom, J.A., "Watermarking Applications and their Properties." Proc. of IEEE Int. Conference on Information Technology, Las Vegas. (March 2000): pp. 6-10.

[9] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M.M., "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications." IEEE Journal On Selected Areas in Communications. Vol. 16, No. 4, (May 1998): pp. 573-586.

[10] Voloshynovskiy S. *et al.,* "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks." IEEE Communication Magazine. Vol. 39. No. 8, (August 2001): pp. 118-126.

[11] Gordy, J.D., and Bruton, L.T., "Performance Evaluation of Digital Audio Watermarking Algorithm." Proc .of 43rd IEEE Midwest Symposium on Circuits and Systems. Vol. 1, (August 2000): pp 456-459.

[12] Ruanaidh, J.J.K.O', Dowling, W.J., and Boland, F.M., "Phase Watermarking of Digital Images." Proc. of IEEE Int. Conference on Image Processing, Lausanne, Switzerland. Vol. 3, (September 16-19, 1996): pp. 239-242.

[13] Ruanaidh, J.J.K.O', and Pun, T., "Rotation, Scale and Translation Invariant Digital Image Watermarking." Proc. of IEEE Int. Conference on Image Processing, Santa Barbara, CA, USA. Vol. 1, (October 1997): pp. 536-539.

[14] Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia." Proc. of IEEE Int. Conference on Image Processing. Vol. 6, (December 1997): pp. 1673-1687.

[15] Boland, F.M., Ruanaidh, J. J. K. O´, and Dautzenberg, C. "Watermarking Digital Images for Copyright Protection." Proc. of IEEE Int. Conference on Image Processing and its Application, Edinburgh, U.K. (July 1995): pp. 321-326.

[16] Barni, M., Bartolini, F., Cappellini, V., and Piva, A., "A DCT Domain System for Robust Image Watermarking." Signal Processing Archive. Vol. 66, No. 3, (May 1998): pp. 357-372.

[17] Burgett, S., Koch, E., and Zhao, J., "Copyright Labeling of Digitized Image Data." IEEE Communication Magazine. Vol. 36, (March 1998): pp. 94-100.

[18] Bors, A.G., and Pitas, I., "Image Watermarking Using DCT Domain Constraints." Proc. of IEEE Int. Conference on Image Processing, Lausanne, Switzerland. Vol. 3, (September 16–19, 1996): pp. 231-234.

[19] Swanson, M.D., Zhu B., and Tewfik, **A.**H., "Transparent Robust Image Watermarking." Proc. of IEEE Int. Conference on Image Processing. Vol. 3, (1997): pp. 211-214.

[20] Tao, B., and Dickinson, B., "Adaptive Watermarking in the DCT Domain." Proc. of IEEE Int. Conference on Acoustics, Speech and Signal Processing, Munich, Germany. Vol. 4, (1997): pp. 2985-2988.

[21] Podilchuk, C.I., and Zeng, W., "Perceptual Watermarking of Still Images." IEEE Workshop on Multimedia Signal Processing, Princeton, New Jersey. (June 23-25, 1997): pp. 363-368.

[22] Wu, J., and Xie, J., "Adaptive Image Watermarking Scheme Based on HVS and Fuzzy Clustering Theory." Proc. of IEEE int. Conference on Neural Network and Signal Processing, Nanjing, China. (December 14-17, 2003): pp. 1493-1496.

[23] Zhang, W., Zhu, W., and Fu, Y., "An Adaptive Digital Watermarking Approach." Proc. of IEEE int. Conference on Mechatronics and Automation, Chengdu, China. (August 2004): pp. 690-695.

[24] Pu, Y., *et el.,* "A Public Adaptive Watermark Algorithm for Color Images Based on Principal Component Analysis of Generalized Hebb." Proc. of IEEE int. Conference on Information Acquisition. (2004): pp. 690-695.

[25] Xia, X.-G., Boncelet, C.G., and Arce, G.R., "A Multiresolution Watermark for Digital Images." Proc. of IEEE Int. Conference. on Image Processing, Santa Barbara, CA, USA. Vol.3, (October 26-29, 1997): pp. 548-551.

[26] Podilchuk, C.I., and Zeng, W., "Image Adaptive Watermarking Using Visual Models." IEEE Journal on Selected Areas in Communication. Vol. 16, No. 4, (May 1998): pp. 525-539.

[27] Hsieh, M.-S., Tseng D.-C., and Huang Y.-H., "Hiding Digital Watermarks Using Multiresolution Wavelet Transform." IEEE Transaction on Industrial Electronics. Vol. 48, No. 5, (October 2001): pp.875-882.

[28] Kundur, D., and Hatzinakos D., "Digital Watermarking Using Multiresolution Wavelet Decomposition." Proc. of IEEE Int. Conference on Acoustics, Speech and Signal Processing. Vol. 5, (1998): pp. 2969-2972.

[29] Barni, M., Bartolini F., and Piva, A., "Improved Wavelet-Based Watermarking Through Pixel-wise Masking." IEEE Transaction on Image Processing. Vol. 10, No. 5, (May 2001): pp. 783-791.

[30] Kang X., Huang J., Shi Y.Q., and Lin Y., "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression." IEEE Transaction on Circuits and Systems for Video Technology. Vol. 13, No. 8, (August 2003): pp. 776-786.

[31] Wu, J., and Xie, J., "Blind Wavelet-Based Watermarking Scheme Using Fuzzy Clustering Theory." Proc. of IEEE int. Conference on Neural Network and Signal Processing, Nanjing, China. (December 14-17, 2003): pp. 1521-1524.

[32] Guannan, Z., Shuxun, W., and Quan, W., "An Adaptive Block-Based Blind Watermarking Algorithm." Proc. of IEEE int. Conference on Signal Processing. (2004): pp. 2294-2297.

[33] Mallat, S.G., "Multifrequency Channel Decompositions of Images and Wavelet Models." IEEE Transaction on Acoustics, Speech and Signal Processing. Vol. 37, No. 12,(December 1989): pp. 2091-2110.

[34] Wilson, T.A., Rogers S.K., and Myers L.R., "Perceptual-based hyperspectral image fusion using multiresolutional analysis." Optical Engineering. Vol. 34, (November 1995): pp. 3154-3164.

[35] Levine, M. D. Vision in Man and Machine. New York: McGraw-Hill, Toronto, 1985.

[36] Kundur, D., and Hatzinakos D., "Toward Robust Logo Watermarking Using Multiresolution Image Fusion Principles." IEEE Transaction on Multimedia. Vol. 6, No. 1, (February 2004): pp. 185-197.